

## 明 細 書

信号処理システム

5

## 技術分野

この発明は、例えばパーソナルコンピュータと接続されたドライブによってディスクメディア例えばDVD (Digital Versatile Disc)規格のディスクにコンテンツを記録し、また、ディスクメディアからコンテンツを再生する場合に適用される信号処理システム、記録再生装置、記録方法、記録方法のプログラム並びに記録媒体に関する。

10

## 背景技術

近年開発されたDVD等の記録媒体では、1枚の媒体に例えば映画1本分の大量のデータをデジタル情報として記録することが可能である。このように、大量の映像情報等をデジタル情報として記録することが可能になると、不正コピーを防止して著作権者の保護を図ることが益々重要になってくる。

15

例えば、DVD-Videoでは、CSS (Content Scramble System)と呼ばれる著作権保護技術が採用されている。DVDに関する著作権保護の方法に関しては、下記の文献1および文献2説明されている。

20

(文献1)

「2部知的財産権保護 ソフトウェア復号のカギを握る不正コピー防止技術にメド」, 日経エレクトロニクス 1997. 8. 18, p. 110-119

25 (文献2)

山田, 「DVDを起点に著作権保護空間を広げる」, 日経エレクトロニ

クス 2001.8.13, p.143-153

第1図は、これらの文献に説明されているCSS方式の概要を示す。  
この方式の場合には、3つの暗号化鍵データが使用される。3つの暗号  
化鍵データは、CSS鍵発行センターが発行するマスターキーと、著作  
5 権者等が決めるディスクキーおよびタイトルキーである。マスターキー  
は、秘密とされ、メーカー毎に異なる固定の値の鍵であり、ディスクキ  
ーは、ディスク毎に異なる値の鍵である。何れのマスターキーでも復号  
できるようなディスクキーのセットが作成され、そのセットがディスク  
に格納される。ディスクキーをディスクに格納する場合に暗号化されて  
10 おり、セキュアドディスクキーと呼ばれる。

ビデオデータ、オーディオデータなどのコンテンツデータを圧縮した  
MPEG (Moving Picture coding Experts Group) データ1に対して、  
そのコンテンツに割当てられた暗号化鍵であるタイトルキー2を用意す  
る。さらに、1枚毎のディスクに割当てられた暗号化鍵であるディスク  
15 キー3を用意する。そして、暗号化の管理を行う鍵発行センター4では、  
そのセンター4が管理するマスターキー5を使用して、ディスクキー3を  
暗号化回路（以下、適宜エンクリプタと称する）6によって暗号化し、  
さらにディスクキー3を使用してタイトルキー2をエンクリプタ7によ  
って暗号化する。そして、MPEGデータ1に対してタイトルキー2に  
20 よってスクランブラ8で暗号化する。

暗号化されたコンテンツデータ（以下、スクランブルドMPEGデー  
タまたはスクランブルドコンテンツと適宜称する）9と、暗号化された  
ディスクキー（以下、セキュアドディスクキーと適宜称する）10と、  
暗号化されたタイトルキー（以下、暗号化タイトルキーと適宜称する）  
25 11とがDVD-Videoディスク製造時にDVD-Videoディスク12に  
記録される。セキュアドディスクキーがディスク12のリードインエリ

アの所定の位置に記録され、暗号化タイトルキーがセクタ構造化されたコンテンツデータの各セクタに記録される。これらのセキュアドディスクキーおよび暗号化タイトルキーは、著作権保護システム用の鍵情報であり、両者をまとめてCSSキーと称する。

- 5 第2図に示すように、DVDプレイヤーによってDVD-Videoディスク12が再生され、スクランブルDMPEGデータ9、セキュアドディスクキー10および暗号化タイトルキー11が再生され、DVDプレイヤー21に読み込まれる。DVDプレイヤー21では、マスターキー22を使用して暗号化の復号回路（以下、適宜デクリプタと称する）23
- 10 3によってディスクキーを復号し、復号したディスクキーを使用してデクリプタ24によってタイトルキーを復号し、復号したタイトルキーを使用してデスクランブラ25によってMP EGデータを復号する。MP EGデコーダ26によってオーディオ／ビジュアルデータ27が復号される。
- 15 第3図は、ディスク再生時にプレイヤーが最初に読み取り出す領域であるリードインエリアのデータ構成を示す。リードインエリアは、物理的なセクタ番号が0h（hは16進数表記であることを示す記号：以下同じ）から30000hのセクタまで使用され、最初に全ての値が0のエリアが配置され、その後に参照用コードが配置され、再度全ての値が
- 20 0のエリアが配置され、その後にコントロールデータエリアが設けられている。その後、さらに全ての値が0のエリアがあり、セクタ番号30000hからコンテンツデータが記録されるメインデータエリアとなる。
- 25 コントロールデータエリアは、最初の1セクタ（セクタ0）に物理フォーマット情報が配置され、次の1セクタ（セクタ1）にディスク製造情報が配置され、次の14セクタ（セクタ2～15）にコンテンツ供給者の情報が配置される。このセクタ0からセクタ15までの16セクタ

の情報が、コントロールデータエリアに繰り返し配置される。そして、コンテンツ・プロバイダー・インフォメーション（コンテンツ供給者の情報）が配置される区間に、そのディスクに特有のセキュアドディスクキーが配置される。

- 5      また、タイトルキーが記録される構造について、第4図に示すセクタ構造例に基づいて説明すると、コンテンツデータなどのメインデータが記録されるそれぞれのセクタは、2064バイトで構成される。この2064バイトの内の先頭の4バイトがセクタ番号などを示すIDデータとされ、続いた2バイトがIDデータエラー検出用データIEDとされ、  
10      さらに次の6バイトがコピー管理用データRSVとされ、このコピー管理用データRSVの中に暗号化タイトルキーが配置される。そして、コピー管理用データに続いた2048（2K）バイトがコンテンツデータなどが記録されるメインデータの記録エリアとされる。さらに、最後の4バイトには、このセクタ全体のエラー検出用データEDCが配置さ  
15      れる。

- このようにディスクキーとタイトルキーを使用して暗号化されてデータが格納されるディスクは、基本的に再生専用のディスクであるが、DVD規格の中には、記録が可能な規格のディスクも存在する。例えば、DVD-RW／-R規格のディスク、DVD+RW／+R規格のディスクは、データの記録が可能であり、いわゆるビットバイビットコピー（bit by bit copy）と称される他の媒体から再生したデジタルデータを、  
20      そのまま別の媒体に記録させる処理を行って、DVD-Videoから読出したデータを、これらの規格のディスクにそのまま記録させることで、DVD-Videoディスクのビデオデータなどのコンテンツデータの  
25      コピーを不正に作成することができる。しかしながら、上述したディスクキーとタイトルキーが用意されることで、不正にコピーされたビデオデー



タなどのコンテンツデータが復号できないようになされる。

この不正にコピーされたディスクでは、暗号化からの正しい復号ができない点について、第5図を参照して説明する。まず、セキュアドディスクキーと暗号化タイトルキーとが上述した配置で記録されたDVD-VideoのディスクDaを用意して、そのディスクDaをユーザが再生する。プレイヤー内では、そのディスクの最内周部のリードインエリアからセキュアドディスクキーが得られ、コンテンツデータが記録されたセクタからは、暗号化タイトルキーが得られる。セキュアドディスクキーがマスターキーによって復号され、暗号化タイトルキーがディスクキーによって復号される。タイトルキーによって、スクランブルDMPEGデータが復号され、オーディオ/ビジュアルデータが得られる。

このDVD-VideoのディスクDaに記録されたコンテンツデータをDVD-RW/R規格のディスクDbに、ビットバイビットコピーで記録させることをユーザが実行したとする。ここで、ディスクDbは、リードインエリアの一部がディスク製造時にビットで書込み済みのエリアとしてあり、その書込み済みのエリアに、そのディスクDbに割当てられたディスクキー又は無効なキーが予め書き込んである。

したがって、ディスクDbのデータ記録可能エリアに、DVD-VideoのディスクDaから読出したコンテンツデータをそのまま記録させたDVD-R/RW規格のディスクDb'をユーザが制作した場合、ディスクDb'は、元のディスクDaとはディスクキーが異なっている。ディスクキーが元のディスクDaとは異なるために、コピーされたディスクDb'をユーザが再生しようとしても、プレイヤーでは、正しく復号することができず、結果的に不正コピーが防止されることになる。

なお、ここでは主としてDVD-Videoのディスクに適用されるCSS方式の場合について説明したが、DVDオーディオのディスクなどに

適用されるスクランブル方式であるC P P M (Content Protection for Pre-Recorded)方式の場合にも、基本的な原理は同じである。

第6図は、C S S方式で記録されたR O Mディスク例えばD V D - V i  
deoディスクを再生するP Cとドライブでのディスクキーとタイトルキ  
5 ーの取り出し方、およびスクランブルデータのデスクランブルの方法を  
示すものである。第6図において、参照符号3 1がC S Sで記録された  
D V D - Videoディスクを再生する再生装置としてのD V Dドライブを  
示す。参照符号4 1がデータ処理装置としてのP Cを示す。P C 4 1に  
対してD V Dプレイヤーアプリケーションソフトウェアがインストール  
10 される。

D V Dドライブ3 1とP C 4 1との間が標準的なインターフェースで  
接続されている。インターフェースは、A T A P I (AT Attachment wi  
th Packet Interface), S C S I (Small Computer System Interface),  
U S B (Universal Serial Bus), I E E E (Institute of Electrical  
15 and Electronics Engineers) 1 3 9 4等である。

D V Dドライブ3 1には、認証部3 2、バスエンクリプタ3 3および  
3 4が備えられている。P C 4 1には、認証部4 2、バスエンクリプタ  
4 3および4 4が備えられている。認証部3 2および認証部4 2は、相  
互認証を行い、認証動作の度に異なるセッションキー（バスキーとも呼  
20 ばれる）K sを生成する。また、P C 4 1には、マスターキー4 5、デ  
クリプタ4 6および4 7、デスクランブラ4 8が備えられ、デスクラン  
ブラ4 8から得られたM P E GデータがM P E Gデコーダ4 9で復号さ  
れることによってオーディオ／ビジュアルデータ5 0が得られる。

なお、認証動作は、電源のO N後のディスク検出時並びにディスクの  
25 交換時には、必ず行われる。また、記録ボタンを押して記録動作を行う  
場合、並びに再生ボタンを押して再生動作を行う場合に、認証動作を行

うようにしても良い。一例として、記録ボタンまたは再生ボタンを押した時に、認証がなされる。

DVD-Videoディスクから得られたスクランブルDMPEGデータ  
9、セキュアドディスクキーが10、暗号化タイトルキー11がDVD  
5 ドライブ31に読み込まれる。コンテンツデータが記録されたセクタからは、暗号化タイトルキーが得られる。セキュアドディスクキーがマスターキーによって復号され、暗号化タイトルキーがディスクキーによって復号される。タイトルキーによって、スクランブルDMPEGデータが復号され、オーディオ/ビジュアルデータが得られる。

10 第7図は、第6図に示す現行のシステムにおいて、DVDドライブ31とPC41との間の信号の授受の手順を示す。PC41がDVDドライブ31に対してコマンドを送り、DVDドライブ31がコマンドに回答した動作を行う。DVD-Videoディスクの挿入等でシーケンスが開始し、最初に認証シーケンスAKE (Authentication and Key Exchange)  
15 e) (ステップS1) がなされる。相互認証が成立すると、セッションキーKsをDVDドライブ31とPC41が共有する。認証が成立しなかった場合では、処理が中断する。

次に、PC41からの要求に応じてDVD-Videoディスク12上のコンテンツデータゾーンがシークされ、読み出される(ステップS2)。  
20 次のステップS3において、セキュアドディスクキーをPC41がドライブ31に対して要求し、ドライブ31がDVD-Videoディスク12からセキュアドディスクキーを読み取る(ステップS4, S5)。セキュアドディスクキーがセッションキーKsを使用してバスエンクリプタ33によって暗号化される。Ksで暗号化されたセキュアドディスクキーがドライブ31からPC41に戻される(ステップS6)。  
25

次に、暗号化タイトルキーおよびコピー世代管理情報CGMS (Copy

Generation Managemrnt System)をP C 4 1がドライブ3 1に対して要求し(ステップS 7)、ドライブ3 1がDVD-Videoディスク1 2から暗号化タイトルキーおよびCGMSを読み取る(ステップS 8, S 9)。暗号化タイトルキーおよびCGMSがセッションキーK sを使用してバスエンクリプタ3 4によって暗号化される。K sで暗号化された暗号化タイトルキーおよびCGMSがドライブ3 1からP C 4 1に戻される(ステップS 1 0)。

次に、スクランブルドコンテンツ(スクランブルドMPEGデータと同一の意味である)をP C 4 1がドライブ3 1に対して要求し(ステップS 1 1)、ドライブ3 1がDVD-Videoディスク1 2からスクランブルドコンテンツを読み取る(ステップS 1 2, S 1 3)。スクランブルドコンテンツがドライブ3 1からP C 4 1に戻される(ステップS 1 4)。

上述したCSS方式は、DVD-ROMメディアに対する適用のみが認可されており、DVD-R、DVD-RW、DVD+R、DVD+RW等の記録型DVDでのCSS方式の利用がCSS契約によって禁止されている。したがって、CSS方式で著作権保護されたDVD-Videoの内容を記録型DVDへのまるごとコピー(ビットバイビットコピー)することは、CSS契約上では、認められた行為ではない。

しかしながら、CSSの暗号方式が破られる事態が発生した。CSSの暗号化を解除してDVD-Videoの内容を簡単にハードディスクにコピーすることを可能とする「DeCSS」と呼ばれるソフトウェアがインターネット上で配布された。「DeCSS」が出現した背景には、本来耐タンパー化が義務付けられているはずのCSS復号用の鍵データを耐タンパー化しないまま設計された再生ソフトウェアがリバースエンジニアされて鍵データが解読されたことによって、連鎖的にCSSアルゴ

リズム全体が解読された経緯がある。

CSSの後に、DVD-Audio等のDVD-ROMの著作権保護技術であるCPPM(Content Protection for Pre-Recorded Media)、並びに記録型DVD、メモリカードに関する著作権保護技術CPRM(Content Protection for Recordable Media)が提案されている。これらの方式は、コンテンツの暗号化や管理情報の格納等に問題が生じたときに、システムを更新でき、また、データをまるごとコピーしても再生を制限できる特徴を有している。すなわち、CPRMは、ビットバイビットコピーを禁止するため、リードインエリアの鍵情報を記録するエリアを予め記録済みとしている。CPRMは、ライセンス管理者である米4C Entity, LLCが配布する下記の資料(文献3)に説明されている。

(文献3)

"Content Protection for Recordable Media Specification DVD Book", インターネット<URL: <http://www.4Centity.com/>>

しかしながら、市場に既に大量に供給されたDVDプレイヤーは、後から規格化されたCPRMへ対応しておらず、また、CPRM規格化後のDVDプレイヤーもコスト的な理由からCPRMへ対応しないものが殆どである。したがって、既存のDVD-Videoプレイヤーとの互換性を考慮すると、CPRMを採用しにくい。一方、BSデジタル放送および地上波デジタル放送の実用化と共に、放送コンテンツの著作権の保護のために、放送の暗号化記録に対する必要性が増大している。

「DeCSS」が出現してきた状況において、コンテンツの著作権を保護する他の方法として、予めオーディオ/ビジュアルデータに電子透かし情報を埋め込んでおくことが考えられる。電子透かし情報は、コピー後でも保存されるので、再生時に電子透かし情報を検出して再生を禁止することが可能である。

しかしながら、電子透かし情報を埋め込む方法は、いくつかの問題があり、実際に行うことが難しい。すなわち、オーディオ／ビジュアル情報の単位より小さい単位でのランダムアクセスが可能なこと、ATAPIという一つのチャンネルを介して読み出しデータと書き込みデータが  
5 流れること、電子透かし情報の検出のための回路規模が大きく、コスト負担が重いこと、電子透かし情報の検出のための処理時間が長くなるために、ドライブ本来の書き込み時間や読み出し時間の短縮化の妨げとなること等が存在する。

電子透かし情報を使用しないで、DVD-Videoの違法なコピーを防止  
10 止するために、ドライブが読み出しデータフィルタおよび書き込みデータフィルタを備えるものが提案されている。読み出しデータフィルタは、ディスクから読み出したデータがDVD-Videoデータのビデオ、オーディオ、サブピクチャの何れかの種類のパックであれば、当該パックに対してマスク処理を行い、それ以外の制御情報のパックであれば、マス  
15 ク処理を行わずに、パックをバッファメモリへ転送する。マスク処理とは、対象のデータを無効データ例えば全てゼロのデータに置き換える処理を意味する。このようにしてDVD-Videoコンテンツの違法な再生を防止できる。

書き込みデータフィルタは、PCから転送されてきたパックのパック  
20 ヘッダを検出してパックの種類を判定し、データがDVD-Videoデータのビデオ、オーディオ、サブピクチャの何れかの種類のパックであれば、当該パックに対してマスク処理を行い、それ以外の制御情報のパックであれば、マスク処理を行わずに、パックをDVDエンコーダへ転送する。したがって、PCによってDVD-Videoのコンテンツが違法に  
25 コピーされることを防止することができる。

この方法は、PCと書き込み可能なDVDディスクとを利用した違法

な再生および記録をDVD-Videoのフォーマットに基づいて防止することができる。しかしながら、DVD-Videoのフォーマットのデータの記録再生が一切できなくなる問題がある。この点を考慮して、PCとドライブとの間で認証を行い、認証が成立しない時には、上述したようなDVDドライブでコンテンツデータのマスク処理を行うモードとし、  
5 認証が成立した時には、コンテンツデータの暗号化／復号を行うモードとする方法が提案されている。この方法は、DVD-Videoディスクを再生することを可能とする。しかしながら、先に提案されている方法では、書き込み時には、コンテンツデータに対してスクランブルをかけて  
10 いない。

書き込みデータに対してスクランブルをかけていないために、既存のDVD-VideoのプレイヤーのCSSを利用することができず、また、記録されたコンテンツデータが著作権が保護されたコンテンツとならない問題があった。たとえCSSの暗号化を破る「DeCSS」ソフトウェアが存在している状況下でも、記録されているコンテンツが正規の  
15 ライセンス機関の承認を受けたCSSでもってスクランブルがかけられていることは、著作権が保護されるコンテンツであることを明示する上で重要である。

よって、この発明の目的は、ドライブによって書き込み時に著作権保護技術例えばCSSによって、書き込みデータを保護し、書き込まれた  
20 データが保護の対象であることを明示することが可能な信号処理システム、記録再生装置、記録方法、記録方法のプログラム並びに記録媒体を提供することにある。

また、この発明は、著作権保護技術を一般ユーザの所有するPCのアプリケーションとして搭載する場合に、一般ユーザによる著作権保護技術の書き込みソフトウェアを作成させないようにできる信号処理システ  
25

ム、記録再生装置、記録方法、記録方法のプログラム並びに記録媒体を提供することにある。

#### 発明の開示

- 5 上述した課題を解決するために、この発明の第1の態様は、記録媒体から情報を読み出し、記録媒体に情報を記録する記録再生装置と、記録再生装置が伝達手段を介して接続される情報処理装置とを備え、管理機構が管理する第1の暗号化鍵と、記録媒体固有の第2の暗号化鍵と、記録の度に生成される第3の暗号化鍵とを使用したコンテンツ情報暗号化
- 10 方法で暗号化されたコンテンツ情報を記録媒体に記録する信号処理システムであって、
- 記録再生装置は、
- 第1の暗号化鍵を保持する保持手段と、
- 記録媒体に暗号化されて記録されている第2の暗号化鍵を再生し、第
- 15 1の暗号化鍵で復号する第2の暗号化鍵復号手段と、
- 第3の暗号化鍵を生成する第3の暗号化鍵生成手段と、
- 第3の暗号化鍵を復号された第2の暗号化鍵で暗号化する暗号化手段と、
- 情報処理装置との間の認証を行い、認証成立時にセッションキーを生
- 20 成する認証手段と、
- 暗号化されて記録されている第2の暗号化鍵をセッションキーによってバス暗号化して情報処理装置に伝送する第1のバス暗号化手段と、
- 暗号化された第3の暗号化鍵をセッションキーによってバス暗号化して情報処理装置に伝送する第2のバス暗号化手段と、
- 25 情報処理装置からの暗号化およびバス暗号化されたコンテンツ情報をバス復号するバス復号手段と、



暗号化された第 3 の暗号化鍵と、暗号化されたコンテンツ情報を記録媒体に記録する記録手段とを有し、

情報処理装置は、

第 1 の暗号化鍵を保持する保持手段と、

- 5     記録再生装置との間の認証を行い、認証成立時にセッションキーを生成する認証手段と、

バス暗号化された第 2 の暗号化鍵をセッションキーによってバス復号して暗号化された第 2 の暗号化鍵を復号する第 1 のバス復号手段と、

暗号化された第 2 の暗号化鍵を第 1 の暗号化鍵で復号する復号手段と、

- 10    バス暗号化された第 3 の暗号化鍵をセッションキーによってバス復号して暗号化された第 3 の暗号化鍵を復号する第 2 のバス復号化手段と、

暗号化された第 3 の暗号化鍵を第 2 の暗号化鍵で復号する復号手段と、

記録再生装置に対して伝送するコンテンツ情報を第 3 の暗号化で暗号化する暗号化手段と、

- 15    暗号化されたコンテンツ情報をセッションキーでバス暗号化して記録再生装置に送出するバス暗号化手段とを有する信号処理システムである。

この発明の第 2 の態様は、記録媒体から情報を読み出し、記録媒体に情報を記録する記録再生装置と、記録再生装置が伝達手段を介して接続される情報処理装置とを備え、管理機構が管理する第 1 の暗号化鍵と、

- 20    記録媒体固有の第 2 の暗号化鍵と、記録の度に生成される第 3 の暗号化鍵とを使用したコンテンツ情報暗号化方法で暗号化されたコンテンツ情報を記録媒体に記録する信号処理システムであって、

記録再生装置は、

第 1 の暗号化鍵を保持する保持手段と、

- 25    第 2 の暗号化鍵を生成する第 2 の暗号化鍵生成手段と、

生成された第 2 の暗号化鍵を第 1 の暗号化鍵で暗号化する暗号化手段

と、

第 3 の暗号化鍵を生成する第 3 の暗号化鍵生成手段と、

生成された第 2 の暗号化鍵で第 3 の暗号化鍵を暗号化する暗号化手段

と、

- 5 情報処理装置との間の認証を行い、認証成立時にセッションキーを生成する認証手段と、

暗号化された第 2 の暗号化鍵をセッションキーによってバス暗号化して情報処理装置に伝送する第 1 のバス暗号化手段と、

- 10 暗号化された第 3 の暗号化鍵をセッションキーによってバス暗号化して情報処理装置に伝送する第 2 のバス暗号化手段と、

情報処理装置からの暗号化およびバス暗号化されたコンテンツ情報をバス復号するバス復号手段と、

暗号化された第 2 の暗号化鍵と、暗号化された第 3 の暗号化鍵と、暗号化されたコンテンツ情報を記録媒体に記録する記録手段とを有し、

- 15 情報処理装置は、

第 1 の暗号化鍵を保持する保持手段と、

記録再生装置との間の認証を行い、認証成立時にセッションキーを生成する認証手段と、

- 20 バス暗号化された第 2 の暗号化鍵をセッションキーによってバス復号して暗号化された第 2 の暗号化鍵を復号する第 1 のバス復号手段と、

暗号化された第 2 の暗号化鍵を第 1 の暗号化鍵で復号する復号手段と、

バス暗号化された第 3 の暗号化鍵をセッションキーによってバス復号して暗号化された第 3 の暗号化鍵を復号する第 2 のバス復号化手段と、

暗号化された第 3 の暗号化鍵を第 2 の暗号化鍵で復号する復号手段と、

- 25 記録再生装置に対して伝送するコンテンツ情報を第 3 の暗号化で暗号化する暗号化手段と、

暗号化されたコンテンツ情報をセッションキーでバス暗号化して記録再生装置に送出するバス暗号化手段とを有する信号処理システムである。

この発明の第 3 の態様は、記録媒体から情報を読み出し、記録媒体に情報を記録する記録再生装置と、記録再生装置が伝達手段を介して接続  
5 される情報処理装置とを備え、管理機構が管理する第 1 の暗号化鍵と、記録媒体固有の第 2 の暗号化鍵と、記録の度に生成される第 3 の暗号化鍵とを使用したコンテンツ情報暗号化方法で暗号化されたコンテンツ情報を記録媒体に記録する信号処理システムであって、

記録再生装置は、

10 第 1 の暗号化鍵を保持する保持手段と、  
記録媒体に暗号化されて記録されている第 2 の暗号化鍵を再生し、第 1 の暗号化鍵で復号する第 2 の暗号化鍵復号手段と、  
第 3 の暗号化鍵を生成する第 3 の暗号化鍵生成手段と、  
第 3 の暗号化鍵を復号された第 2 の暗号化鍵で暗号化する暗号化手段  
15 と、

情報処理装置との間の認証を行い、認証成立時にセッションキーを生成する認証手段と、

情報処理装置からのバス暗号化されたコンテンツ情報をバス復号するバス復号手段と、

20 コンテンツ情報を第 3 の暗号化鍵によって暗号化する暗号化手段と、  
暗号化された第 3 の暗号化鍵と、暗号化されたコンテンツ情報を記録媒体に記録する記録手段とを有し、

情報処理装置は、

記録再生装置との間の認証を行い、認証成立時にセッションキーを生成する認証手段と、  
25

記録再生装置に対して伝送するコンテンツ情報をセッションキーでバ

ス暗号化して記録再生装置に送出するバス暗号化手段とを有する信号処理システムである。

この発明の第4の態様は、記録媒体から情報を読み出し、記録媒体に情報を記録する記録再生装置と、記録再生装置が伝達手段を介して接続  
5 される情報処理装置とを備え、管理機構が管理する第1の暗号化鍵と、記録媒体固有の第2の暗号化鍵と、記録の度に生成される第3の暗号化鍵とを使用したコンテンツ情報暗号化方法で暗号化されたコンテンツ情報を記録媒体に記録する信号処理システムであって、

記録再生装置は、

10 第1の暗号化鍵を保持する保持手段と、

第2の暗号化鍵を生成する第2の暗号化鍵生成手段と、

生成された第2の暗号化鍵を第1の暗号化鍵で暗号化する暗号化手段と、

第3の暗号化鍵を生成する第3の暗号化鍵生成手段と、

15 第3の暗号化鍵を生成された第2の暗号化鍵で暗号化する暗号化手段と、

情報処理装置との間の認証を行い、認証成立時にセッションキーを生成する認証手段と、

20 情報処理装置からのバス暗号化されたコンテンツ情報をバス復号するバス復号手段と、

コンテンツ情報を第3の暗号化鍵によって暗号化する暗号化手段と、

暗号化された第2の暗号化鍵と、暗号化された第3の暗号化鍵と、暗号化されたコンテンツ情報を記録媒体に記録する記録手段とを有し、

情報処理装置は、

25 記録再生装置との間の認証を行い、認証成立時にセッションキーを生成する認証手段と、

コンテンツ情報をセッションキーでバス暗号化して記録再生装置に送出するバス暗号化手段とを有する信号処理システムである。

この発明の第 5 の態様は、伝達手段を介して情報処理装置と接続され、記録媒体から情報を読み出し、記録媒体に情報を記録する記録再生装置  
5 であって、管理機構が管理する第 1 の暗号化鍵と、記録媒体固有の第 2 の暗号化鍵と、記録の度に生成される第 3 の暗号化鍵とを使用したコンテンツ情報暗号化方法で暗号化されたコンテンツ情報を記録媒体に記録する記録再生装置であって、

第 1 の暗号化鍵を保持する保持手段と、  
10 記録媒体に暗号化されて記録されている第 2 の暗号化鍵を再生し、第 1 の暗号化鍵で復号する第 2 の暗号化鍵復号手段と、

第 3 の暗号化鍵を生成する第 3 の暗号化鍵生成手段と、

第 3 の暗号化鍵を復号された第 2 の暗号化鍵で暗号化する暗号化手段と、

15 情報処理装置との間の認証を行い、認証成立時にセッションキーを生成する認証手段と、

暗号化されて記録されている第 2 の暗号化鍵をセッションキーによってバス暗号化して情報処理装置に伝送する第 1 のバス暗号化手段と、

暗号化された第 3 の暗号化鍵をセッションキーによってバス暗号化して  
20 情報処理装置に伝送する第 2 のバス暗号化手段と、

情報処理装置からの暗号化およびバス暗号化されたコンテンツ情報をバス復号するバス復号手段と、

暗号化された第 3 の暗号化鍵と、暗号化されたコンテンツ情報を記録媒体に記録する記録手段とを有し、

25 暗号化およびバス暗号化されたコンテンツ情報は、第 3 の暗号化鍵で暗号化され、さらに、暗号化コンテンツ情報を情報処理装置で生成され

たセッションキーでバス暗号化したものである記録再生装置である。

この発明の第 6 の態様は、伝達手段を介して情報処理装置と接続され、記録媒体から情報を読み出し、記録媒体に情報を記録する記録再生装置であって、管理機構が管理する第 1 の暗号化鍵と、記録媒体固有の第 2  
5 の暗号化鍵と、記録の度に生成される第 3 の暗号化鍵とを使用したコンテンツ情報暗号化方法で暗号化されたコンテンツ情報を記録媒体に記録する記録再生装置であって、

第 1 の暗号化鍵を保持する保持手段と、

第 2 の暗号化鍵を生成する第 2 の暗号化鍵生成手段と、

10 生成された第 2 の暗号化鍵を第 1 の暗号化鍵で暗号化する暗号化手段と、

第 3 の暗号化鍵を生成する第 3 の暗号化鍵生成手段と、

生成された第 2 の暗号化鍵で第 3 の暗号化鍵を暗号化する暗号化手段と、

15 情報処理装置との間の認証を行い、認証成立時にセッションキーを生成する認証手段と、

暗号化された第 2 の暗号化鍵をセッションキーによってバス暗号化して情報処理装置に伝送する第 1 のバス暗号化手段と、

20 暗号化された第 3 の暗号化鍵をセッションキーによってバス暗号化して情報処理装置に伝送する第 2 のバス暗号化手段と、

情報処理装置からの暗号化およびバス暗号化されたコンテンツ情報をバス復号するバス復号手段と、

暗号化された第 2 の暗号化鍵と、暗号化された第 3 の暗号化鍵と、暗号化されたコンテンツ情報を記録媒体に記録する記録手段とを有し、

25 暗号化およびバス暗号化されたコンテンツ情報は、第 3 の暗号化鍵で暗号化され、さらに、暗号化コンテンツ情報を情報処理装置で生成され

たセッションキーでバス暗号化したものである記録再生装置である。

この発明の第 7 の態様は、伝達手段を介して情報処理装置と接続され、記録媒体から情報を読み出し、記録媒体に情報を記録する記録再生装置であって、管理機構が管理する第 1 の暗号化鍵と、記録媒体固有の第 2  
5 の暗号化鍵と、記録の度に生成される第 3 の暗号化鍵とを使用したコンテンツ情報暗号化方法で暗号化されたコンテンツ情報を記録媒体に記録する記録再生装置であって、

第 1 の暗号化鍵を保持する保持手段と、

記録媒体に暗号化されて記録されている第 2 の暗号化鍵を再生し、第  
10 1 の暗号化鍵で復号する第 2 の暗号化鍵復号手段と、

第 3 の暗号化鍵を生成する第 3 の暗号化鍵生成手段と、

第 3 の暗号化鍵を復号された第 2 の暗号化鍵で暗号化する暗号化手段  
と、

情報処理装置との間の認証を行い、認証成立時にセッションキーを生  
15 成する認証手段と、

情報処理装置からのバス暗号化されたコンテンツ情報をバス復号する  
バス復号手段と、

コンテンツ情報を第 3 の暗号化鍵によって暗号化する暗号化手段と、

暗号化された第 3 の暗号化鍵と、暗号化されたコンテンツ情報を記録  
20 媒体に記録する記録手段とを有し、

バス暗号化されたコンテンツ情報は、暗号化コンテンツ情報を情報処理装置で生成されたセッションキーでバス暗号化したものである記録再生装置である。

この発明の第 8 の態様は、伝達手段を介して情報処理装置と接続され、  
25 記録媒体から情報を読み出し、記録媒体に情報を記録する記録再生装置であって、管理機構が管理する第 1 の暗号化鍵と、記録媒体固有の第 2

の暗号化鍵と、記録の度に生成される第 3 の暗号化鍵とを使用したコンテンツ情報暗号化方法で暗号化されたコンテンツ情報を記録媒体に記録する記録再生装置であって、

第 1 の暗号化鍵を保持する保持手段と、

5 第 2 の暗号化鍵を生成する第 2 の暗号化鍵生成手段と、

生成された第 2 の暗号化鍵を第 1 の暗号化鍵で暗号化する暗号化手段と、

第 3 の暗号化鍵を生成する第 3 の暗号化鍵生成手段と、

10 第 3 の暗号化鍵を生成された第 2 の暗号化鍵で暗号化する暗号化手段と、

情報処理装置との間の認証を行い、認証成立時にセッションキーを生成する認証手段と、

情報処理装置からのバス暗号化されたコンテンツ情報をバス復号するバス復号手段と、

15 コンテンツ情報を第 3 の暗号化鍵によって暗号化する暗号化手段と、

暗号化された第 2 の暗号化鍵と、暗号化された第 3 の暗号化鍵と、暗号化されたコンテンツ情報を記録媒体に記録する記録手段とを有し、

バス暗号化されたコンテンツ情報は、暗号化コンテンツ情報を情報処理装置で生成されたセッションキーでバス暗号化したものである記録再生装置である。

この発明の第 9 の態様は、記録媒体から情報を読み出し、記録媒体に情報を記録する記録再生装置と、記録再生装置が伝達ステップを介して接続される情報処理装置とを備え、管理機構が管理する第 1 の暗号化鍵と、記録媒体固有の第 2 の暗号化鍵と、記録の度に生成される第 3 の暗号化鍵とを使用したコンテンツ情報暗号化方法で暗号化されたコンテンツ情報を記録媒体に記録する記録方法であって、



記録再生装置は、

第 1 の暗号化鍵を保持する保持ステップと、

記録媒体に暗号化されて記録されている第 2 の暗号化鍵を再生し、第 1 の暗号化鍵で復号する第 2 の暗号化鍵復号ステップと、

5 第 3 の暗号化鍵を生成する第 3 の暗号化鍵生成ステップと、

第 3 の暗号化鍵を復号された第 2 の暗号化鍵で暗号化する暗号化ステップと、

情報処理装置との間の認証を行い、認証成立時にセッションキーを生成する認証ステップと、

10 暗号化されて記録されている第 2 の暗号化鍵をセッションキーによってバス暗号化して情報処理装置に伝送する第 1 のバス暗号化ステップと、  
暗号化された第 3 の暗号化鍵をセッションキーによってバス暗号化して情報処理装置に伝送する第 2 のバス暗号化ステップと、

情報処理装置からの暗号化およびバス暗号化されたコンテンツ情報を  
15 バス復号するバス復号ステップと、

暗号化された第 3 の暗号化鍵と、暗号化されたコンテンツ情報を記録媒体に記録する記録ステップとを実行し、

情報処理装置は、

第 1 の暗号化鍵を保持する保持ステップと、

20 記録再生装置との間の認証を行い、認証成立時にセッションキーを生成する認証ステップと、

バス暗号化された第 2 の暗号化鍵をセッションキーによってバス復号して暗号化された第 2 の暗号化鍵を復号する第 1 のバス復号ステップと、

暗号化された第 2 の暗号化鍵を第 1 の暗号化鍵で復号する復号ステップと、  
25 プと、

バス暗号化された第 3 の暗号化鍵をセッションキーによってバス復号

して暗号化された第 3 の暗号化鍵を復号する第 2 のバス復号化ステップと、

暗号化された第 3 の暗号化鍵を第 2 の暗号化鍵で復号する復号ステップと、

- 5 記録再生装置に対して伝送するコンテンツ情報を第 3 の暗号化で暗号化する暗号化ステップと、

暗号化されたコンテンツ情報をセッションキーでバス暗号化して記録再生装置に送出するバス暗号化ステップとを実行する記録方法である。

- また、この発明は、記録方法のプログラムおよびプログラムが格納された記録媒体である。
- 10

- この発明の第 10 の態様は、記録媒体から情報を読み出し、記録媒体に情報を記録する記録再生装置と、記録再生装置が伝達ステップを介して接続される情報処理装置とを備え、管理機構が管理する第 1 の暗号化鍵と、記録媒体固有の第 2 の暗号化鍵と、記録の度に生成される第 3 の暗号化鍵とを使用したコンテンツ情報暗号化方法で暗号化されたコンテンツ情報を記録媒体に記録する記録方法であって、
- 15

記録再生装置は、

第 1 の暗号化鍵を保持する保持ステップと、

第 2 の暗号化鍵を生成する第 2 の暗号化鍵生成ステップと、

- 20 生成された第 2 の暗号化鍵を第 1 の暗号化鍵で暗号化する暗号化ステップと、

第 3 の暗号化鍵を生成する第 3 の暗号化鍵生成ステップと、

生成された第 2 の暗号化鍵で第 3 の暗号化鍵を暗号化する暗号化ステップと、

- 25 情報処理装置との間の認証を行い、認証成立時にセッションキーを生成する認証ステップと、

暗号化された第 2 の暗号化鍵をセッションキーによってバス暗号化して情報処理装置に伝送する第 1 のバス暗号化ステップと、

暗号化された第 3 の暗号化鍵をセッションキーによってバス暗号化して情報処理装置に伝送する第 2 のバス暗号化ステップと、

- 5      情報処理装置からの暗号化およびバス暗号化されたコンテンツ情報をバス復号するバス復号ステップと、

暗号化された第 2 の暗号化鍵と、暗号化された第 3 の暗号化鍵と、暗号化されたコンテンツ情報を記録媒体に記録する記録ステップとを実行し、

- 10      情報処理装置は、

第 1 の暗号化鍵を保持する保持ステップと、

記録再生装置との間の認証を行い、認証成立時にセッションキーを生成する認証ステップと、

- 15      バス暗号化された第 2 の暗号化鍵をセッションキーによってバス復号して暗号化された第 2 の暗号化鍵を復号する第 1 のバス復号ステップと、  
暗号化された第 2 の暗号化鍵を第 1 の暗号化鍵で復号する復号ステップと、

バス暗号化された第 3 の暗号化鍵をセッションキーによってバス復号して暗号化された第 3 の暗号化鍵を復号する第 2 のバス復号化ステップと、

20      暗号化された第 3 の暗号化鍵を第 2 の暗号化鍵で復号する復号ステップと、

記録再生装置に対して伝送するコンテンツ情報を第 3 の暗号化で暗号化する暗号化ステップと、

- 25      暗号化されたコンテンツ情報をセッションキーでバス暗号化して記録再生装置に送出するバス暗号化ステップとを実行する記録方法である。

また、この発明は、記録方法のプログラムおよびプログラムが格納された記録媒体である。

この発明の第 1 の態様は、記録媒体から情報を読み出し、記録媒体に情報を記録する記録再生装置と、記録再生装置が伝達ステップを介して接続される情報処理装置とを備え、管理機構が管理する第 1 の暗号化鍵と、記録媒体固有の第 2 の暗号化鍵と、記録の度に生成される第 3 の暗号化鍵とを使用したコンテンツ情報暗号化方法で暗号化されたコンテンツ情報を記録媒体に記録する記録方法であって、

記録再生装置は、

第 1 の暗号化鍵を保持する保持ステップと、  
記録媒体に暗号化されて記録されている第 2 の暗号化鍵を再生し、第 1 の暗号化鍵で復号する第 2 の暗号化鍵復号ステップと、

第 3 の暗号化鍵を生成する第 3 の暗号化鍵生成ステップと、

第 3 の暗号化鍵を復号された第 2 の暗号化鍵で暗号化する暗号化ステップと、

情報処理装置との間の認証を行い、認証成立時にセッションキーを生成する認証ステップと、

情報処理装置からのバス暗号化されたコンテンツ情報をバス復号するバス復号ステップと、

コンテンツ情報を第 3 の暗号化鍵によって暗号化する暗号化ステップと、

暗号化された第 3 の暗号化鍵と、暗号化されたコンテンツ情報を記録媒体に記録する記録ステップとを実行し、

情報処理装置は、

記録再生装置との間の認証を行い、認証成立時にセッションキーを生成する認証ステップと、

記録再生装置に対して伝送するコンテンツ情報をセッションキーでバス暗号化して記録再生装置に送出するバス暗号化ステップとを実行する記録方法である。また、この発明は、記録方法のプログラムおよびプログラムが格納された記録媒体である。

- 5      この発明の第 1 2 の態様は、記録媒体から情報を読み出し、記録媒体に情報を記録する記録再生装置と、記録再生装置が伝達ステップを介して接続される情報処理装置とを備え、管理機構が管理する第 1 の暗号化鍵と、記録媒体固有の第 2 の暗号化鍵と、記録の度に生成される第 3 の暗号化鍵とを使用したコンテンツ情報暗号化方法で暗号化されたコンテンツ情報を記録媒体に記録する記録方法であって、
- 10      記録再生装置は、
- 第 1 の暗号化鍵を保持する保持ステップと、
- 第 2 の暗号化鍵を生成する第 2 の暗号化鍵生成ステップと、
- 生成された第 2 の暗号化鍵を第 1 の暗号化鍵で暗号化する暗号化ステップと、
- 15      第 3 の暗号化鍵を生成する第 3 の暗号化鍵生成ステップと、
- 第 3 の暗号化鍵を生成された第 2 の暗号化鍵で暗号化する暗号化ステップと、
- 情報処理装置との間の認証を行い、認証成立時にセッションキーを生成する認証ステップと、
- 20      情報処理装置からのバス暗号化されたコンテンツ情報をバス復号するバス復号ステップと、
- コンテンツ情報を第 3 の暗号化鍵によって暗号化する暗号化ステップと、
- 25      暗号化された第 2 の暗号化鍵と、暗号化された第 3 の暗号化鍵と、暗号化されたコンテンツ情報を記録媒体に記録する記録ステップとを実行

し、

情報処理装置は、

記録再生装置との間の認証を行い、認証成立時にセッションキーを生成する認証ステップと、

- 5     コンテンツ情報をセッションキーでバス暗号化して記録再生装置に送出するバス暗号化ステップとを実行する記録方法である。また、この発明は、記録方法のプログラムおよびプログラムが格納された記録媒体である。

- この発明では、暗号化例えばCSS方式でコンテンツ情報を記録するので、記録されたコンテンツ情報は、著作権が保護されたものであることを明確とできる。すなわち、正規のライセンスを受けない違法な方法で、記録されているコンテンツ情報をコピーしたり、再生すれば、著作権を侵害していると主張することができる。この発明では、記録再生装置内で生成した暗号化鍵を記録再生装置自身がメディア例えばDVDディスクへ書き込むことにより、CSS方式でDVDディスクへ記録をするときに、一般のPCユーザがCSS書き込みソフトウェアを作成できないようにできる。このことにより、正規に許可されたものだけがCSS書き込みアプリケーションを作成できるようになる。
- 10     このことにより、正規に許可されたものだけがCSS書き込みアプリケーションを作成できるようになる。
- 15     このことにより、正規に許可されたものだけがCSS書き込みアプリケーションを作成できるようになる。

- この発明では、記録再生装置内で生成した暗号化鍵を記録再生装置自身がメディアへ書き込むことにより、CPRMのように、鍵情報を予め記録ディスクへ記録済みとする必要がなくなることから、ディスク製造にかかるコストの低下に貢献する。
- 20     このことにより、正規に許可されたものだけがCSS書き込みアプリケーションを作成できるようになる。

- この発明では、PCと記録再生装置の相互認証時の乱数データにメディアタイプを含めることによって、セキュアにメディアタイプを記録再生装置からPCへ伝えることが可能となる。このことから、PCと記録再生装置間の標準化されたインターフェース上でのメディアタイプの改
- 25     このことにより、正規に許可されたものだけがCSS書き込みアプリケーションを作成できるようになる。

ざんや、改造された記録再生装置による成りすまし行為を防止することができる。

この発明では、相互認証時の乱数データにコピー世代管理情報（CGMS）を含めることによって、セキュアにCGMSをPCから記録再生  
5 装置へ伝えることが可能となる。このことから、PCと記録再生装置間の標準化されたインターフェース上でのCGMSの改ざんや、改造されたPCアプリケーションによる成りすまし行為を防止することができる。

この発明では、相互認証が成立しない間は、暗号化鍵のディスクへの書き込みを記録再生装置内のエンコーダLSI (Large Scale Integrat  
10 ed Circuit: 大規模集積回路)で禁止し、その暗号化鍵書き込み禁止機能を相互認証の成立によって解除することにより、一般のユーザによるCSS書き込みソフトウェアの作成を禁止できる。このことにより、正規に許可されたものだけがCSS書き込みアプリケーションを作成できるようになる。

15

#### 図面の簡単な説明

第1図は、CSS方式でROMディスクへ記録する際の鍵情報の関係を示すブロック図である。

第2図は、CSS方式で記録されたROMディスクを再生するDVD  
20 プレーヤー内の鍵情報とスクランブルデータの再生の方法を示すブロック図である。

第3図は、ROMディスクのリードインエリアのデータ構成を示す略線図である。

第4図は、セクタの構成を示す略線図である。

25 第5図は、CSS方式によるコピー防止機能を説明するための略線図である。

第 6 図は、C S S 方式で記録された R O M ディスクを再生する P C とドライブでの鍵情報とスクランブルデータの再生の方法を示すブロック図である。

第 7 図は、第 6 図のシステムにおけるドライブとディスク間のデータの  
5 流れを示す略線図である。

第 8 図は、ディスクキーが書き込み済みの記録型 D V D メディアへ C S S 方式でデータを書き込む際の記録方法の一例を示すブロック図である。

第 9 図は、ディスクキーが書き込み済みでない記録型 D V D メディア  
10 へ C S S 方式でデータを書き込む際の記録方法の一例を示すブロック図である。

第 1 0 図は、ディスクキーが書き込み済みの記録型 D V D メディアへ C S S 方式でデータを書き込む際の記録方法を P C とドライブの組み合わせで実現する場合の一例を示すブロック図である。

第 1 1 図は、第 1 0 図の構成におけるドライブとディスク間のデータの  
15 流れを示す略線図である。

第 1 2 図は、ディスクキーが書き込み済みでない記録型 D V D メディアへ C S S 方式でデータを書き込む際の記録方法を P C とドライブの組み合わせで実現する場合の一例を示すブロック図である。

第 1 3 図は、第 1 2 図の構成におけるドライブとディスク間のデータの  
20 流れを示す略線図である。

第 1 4 図は、第 1 0 図の構成に対してスクランブルデータをバス暗号化して転送するようにした構成を示すブロック図である。

第 1 5 図は、第 1 4 図の構成におけるドライブとディスク間のデータの  
25 流れを示す略線図である。

第 1 6 図は、第 1 2 図の構成に対してスクランブルデータをバス暗号



化して転送するようにした構成を示すブロック図である。

第 17 図は、第 16 図の構成におけるドライブとディスク間のデータの  
の流れを示す略線図である。

5 第 18 図は、この発明の第 1 の実施形態の構成を示すブロック図であ  
る。

第 19 図は、第 18 図の構成におけるドライブとディスク間のデータの  
の流れを示す略線図である。

第 20 図は、この発明の第 2 の実施形態の構成を示すブロック図であ  
る。

10 第 21 図は、第 20 図の構成におけるドライブとディスク間のデータの  
の流れを示す略線図である。

第 22 図は、この発明の第 3 の実施形態の構成を示すブロック図であ  
る。

15 第 23 図は、この発明の第 4 の実施形態の構成を示すブロック図であ  
る。

第 24 図は、第 18 図の構成に対してタイトルキーのマスク制御機構  
を加えたこの発明の第 5 の実施形態の構成を示すブロック図である。

20 第 25 図は、第 20 図の構成に対してディスクキーとタイトルキーの  
マスク制御機構を加えたこの発明の第 6 の実施形態の構成を示すブロッ  
ク図である。

第 26 図は、第 22 図の構成に対してタイトルキーのマスク制御機構  
を加えたこの発明の第 7 の実施形態の構成を示すブロック図である。

25 第 27 図は、第 23 図の構成に対してディスクキーとタイトルキーの  
マスク制御機構を加えたこの発明の第 8 の実施形態の構成を示すブロッ  
ク図である。

第 28 図は、相互認証からセッションキーを生成する仕組みを示して

おり、同時にディスクタイプをセキュアにドライブからP Cへ伝える仕組みを説明する略線図である。

第29図は、ドライブ側におけるディスクタイプの情報の処理を説明するフローチャートである。

- 5 第30図は、P C側におけるディスクタイプの情報の処理を説明するフローチャートである。

第31図は、相互認証からセッションキーを生成する仕組みを示しており、同時にコピー世代管理情報をセキュアにドライブからP Cへ伝える手段を説明する略線図である。

- 10 第32図は、M A C計算やセッションキー生成においてA E Sを利用した場合の例を示すブロック図である。

第33図は、相互認証からセッションキー生成までのドライブ側の処理を示すフローチャートである。

- 15 第34図は、相互認証からセッションキー生成までのP C側の処理を示すフローチャートである。

第35図は、バス暗号化／復号の処理の一例を示すブロック図である。

第36図は、第35図の処理の流れを示すフローチャートである。

第37図は、A Vパックの構造とバス暗号化の対象範囲を説明するための略線図である。

- 20 第38図は、1セクタのデータ構成を示す略線図である。

第39図は、データの記録処理の流れを示す略線図である。

第40図は、マスクコントロールが対象とするデータを説明するための略線図である。

- 25 第41図は、マスクコントロールの構成の一例を示すブロック図である。

第42図は、マスクコントロール内のフィルタの構成の一例（C S S

キー書き込み禁止時)を示すブロック図である。

第43図は、マスクコントロール内のフィルタの構成の一例(CSSキー書き込み禁止解除時)を示すブロック図である。

第44図は、マスクコントロール内のフィルタの構成の応用例を示す  
5 ブロック図である。

第45図は、セッションキーの生成と消滅、およびCSSキーのマスクコントロールの処理を示すフローチャートである。

第46図は、マスターキーの生成方法の他の例を示すブロック図である。

10

発明を実施するための最良の形態

以下、この発明について説明するが、この発明の理解を容易とするために、DVDレコーダでCSS方式による記録を実現するために、考えられるいくつかの例とその場合の問題点について説明する。また、以下の説明では、DVDメディアへの記録についてのみ説明し、再生処理に  
15 ついては、CSS方式による再生処理と同様であるので、その説明を省略する。さらに、本明細書の特許請求の範囲において使用される用語と実施の形態中で使用される用語との対応関係について以下に説明する。

記録媒体：メディア例えばDVDライタブルディスク、記録再生装置：ドライブ、情報処理装置：パーソナルコンピュータ、伝達手段：インターフェース、信号処理システム：メディアを記録再生するドライブとパーソナルコンピュータとがインターフェースを介して接続されるシステムである。  
20

コンテンツ情報：メディアに記録すべき情報例えばオーディオ/ビジュアルデータをコンテンツ情報としている。第1の暗号化鍵：マスター  
25 キーである。第2の暗号化鍵：ディスクキーであり、ディスク上には、

キーである。第2の暗号化鍵：ディスクキーであり、ディスク上には、暗号化されたセキュアドディスクキーとして記録される。第3の暗号化鍵：タイトルキーであり、ディスク上には、暗号化され、暗号化タイトルキーとして記録される。

- 5 第8図は、DVDレコーダ51aにおいて、記録型DVDメディア（以下、ライタブルまたはレコーダブルディスクと適宜称する）13aへCSS方式でコンテンツを書き込む際の記録方法の一例を示す。DVD-Videoと同様にライタブルディスク13aのリードインエリアの決められた場所に予めセキュアドディスクキー10aを書き込み済みとする例である。オーディオ／ビジュアルデータ60がDVDレコーダ51aのMP EGエンコーダ52によって圧縮符号化され、スクランブラ53によってスクランブルされ、スクランブルドMP EGデータ9がライタブルディスク13aに記録される。

- DVDレコーダ51aの内部の乱数生成器（RNG：Random Number Generator）54によりタイトルキーが生成される。タイトルキーは、記録の度に生成され、また、CGMSのステータスが変化した時にも生成される。スクランブラ53は、タイトルキーを使用してMP EGデータをスクランブルする。タイトルキーは、エンクリプタ55で暗号化され、ライタブルディスク13aに暗号化タイトルキー11が記録される。
- 20 記録済みのセキュアドディスクキー10aがデクリプタ56において、マスターキー57によって復号され、ディスクキーが得られる。

- 第9図に示す例は、ライタブルディスクに暗号化鍵情報であるセキュアドディスクキーを予め書き込み済みとしない例である。DVDレコーダ51bが乱数発生器54および58を有し、乱数生成器54および58により、ディスクキーとタイトルキーを生成する。ディスクキーをDVDレコーダ51bがライタブルディスク13bに書き込む。例えばブ

ランクディスクのフォーマッティングの処理によってディスクキーがライタブルディスク 13b に対して書かれる。後からディスクキーを書き込むことによって、ディスクキーを書き込み済みとする第 8 図の方法よりも記録型 DVD メディアの製造コストを下げる事が可能となる。

- 5      第 10 図および第 12 図にそれぞれ示す構成は、CSS 方式でスクランブルされたビデオコンテンツを記録型 DVD メディアへ書き込む機能を、PC とドライブの組み合わせで実現する場合の一例および他の例である。

- 10      これらの図において、参照符号 61 がライタブルディスク 13a または 13b に対してデータを記録し、また、再生する記録再生装置としての DVD ドライブを示す。参照符号 71 がデータ処理装置（ホスト）としての PC を示し、PC 71 に対してアプリケーションソフトウェアがインストールされ、DVD ビデオエンコーダとして PC 71 が機能する。但し、ソフトウェア処理に限定されるものではなく、DVD ビデオエン
- 15      コーダとしてハードウェア構成（基板構成）としても良い。

- 20      DVD ドライブ 61 と PC 71 との間がインターフェースで接続されている。インターフェースは、ATAPI (AT Attachment with Packet Interface), SCSI (Small Computer System Interface), USB (Universal Serial Bus), IEEE (Institute of Electrical and Electronics Engineers) 1394 等である。

- 25      DVD ドライブ 61 には、認証部 62、バスエンクリプタ 63 およびバスデクリプタ 64 が備えられている。PC 71 には、認証部 72、バスデクリプタ 73 およびバスエンクリプタ 74 が備えられている。また、PC 71 には、MPEG エンコーダ 52、スクランブラ 53、乱数発生器 54、エンクリプタ 55、デクリプタ 56 およびマスターキー 57 が備えられている。オーディオ／ビジュアルデータ 60 が MPEG エンコ

データ 52 で、圧縮符号化され、DVD フォーマットの形式のストリームデータに変換される。スクランブラ 53 にてタイトルキーによってスクランブルされて DVD ドライブ 61 にインターフェースを介して供給され、ライタブルディスク 13a 上にスクランブルド MPEG データ 9 が  
5 記録される。

PC 71 の内部の乱数生成器 54 によりタイトルキーが生成される。スクランブラ 53 は、タイトルキーを使用して MPEG データをスクランブルする。タイトルキーは、エンクリプタ 55 で暗号化され、認証が成立した時に生成されるセッションキーで暗号化タイトルキーがバス  
10 エンクリプタ 74 で暗号化される。バスエンクリプタ 74 の出力データが DVD ドライブ 61 のバスデクリプタ 64 に供給され、バスデクリプタ 64 によってセッションキーで暗号化タイトルキーが復号される。ライタブルディスク 13a に暗号化タイトルキー 11 が記録される。

記録済みのセキュアドディスクキー 10a が DVD ドライブ 61 のバス  
15 エンクリプタ 63 において、認証の成立によって生成されたセッションキーによって暗号化される。DVD ドライブ 61 から PC 71 へインターフェースを介して伝送され、バスデクリプタ 73 においてセッションキーを使用して復号される。さらに、デクリプタ 56 において、マスターキー 57 によって復号され、ディスクキーが取得される。

20 第 11 図は、第 10 図に示すシステムにおいて、DVD ドライブ 61 と PC 71 との間の信号の授受の手順を示す。PC 71 が DVD ドライブ 61 に対してコマンドを送り、DVD ドライブ 61 がコマンドに応答した動作を行う。ライタブルディスクの挿入等でシーケンスが開始し、最初に認証シーケンス AKE (ステップ S21) がなされる。認証が成  
25 立すると、セッションキー Ks を DVD ドライブ 61 と PC 71 が共有する。認証が成立しなかった場合では、処理が中断する。

次に、P C 7 1からの要求に応じてD V Dドライブ6 1がライタブルディスク1 3 a上のコントロールデータゾーンをシークし、コントロールデータを読み出す（ステップS 2 2）。次のステップS 2 3において、P C 7 1がセキュアドディスクキーを要求し、D V Dドライブ6 1がセキュアドディスクキーをリードする（ステップS 2 4およびS 2 5）。D V Dドライブ6 1がバスエンクリプタ6 3によってセッションキーK sでセキュアドディスクキーを暗号化し、暗号化されたセキュアドディスクキーをD V Dドライブ6 1がP C 7 1に送る（ステップS 2 6）。P C 7 1のバスデクリプタ7 3がセキュアドディスクキーを復号し、さらに、デクリプタ5 6によってディスクキーを復号する。

次に、ステップS 2 7において、D V Dドライブ6 1が暗号化タイトルキーおよびC G M Sをバスエンクリプタ7 4において、セッションキーK sで暗号化し、D V Dドライブ6 1に対して送出する。さらに、ステップS 2 8において、スクランブラ5 3からのスクランブルドM P E GデータがD V Dドライブ6 1に送出される。D V Dドライブ6 1は、バスデクリプタ6 6においてセッションキーK sで復号した暗号化タイトルキーと、スクランブルドM P E Gデータをライタブルディスク1 3 a上に記録する（ステップS 2 9）。

第1 2図に示す構成例は、第1 0図と比較すると、ライタブルディスク1 3 bに対してセキュアドディスクキーを記録する点で相違している。このため、乱数発生器5 8がP C 7 1に備えられ、ディスクキーが生成される。ディスクキーがエンクリプタ5 9において、マスターキー5 7によって暗号化され、セキュアドディスクキーがバスエンクリプタ7 5において、セッションキーK sによって暗号化される。バスエンクリプタ7 5の出力がD V Dドライブ6 1にインターフェースを介して伝送され、バスデクリプタ6 5において、セッションキーK sによって復号さ

れる。そして、ライタブルディスク 13 b 上にセキュアドディスクキー 10 b が記録される。他の構成は、第 10 図に示すシステムと同様である。

第 13 図は、第 12 図に示すシステムにおける DVD ドライブ 61 と PC 71 との間の信号の授受の手順を示す。前述した第 10 図のシステムにおける第 11 図に示される手順と同様である。但し、バスエンクリプタ 75 において、セッションキー  $K_s$  で暗号化されたセキュアドディスクキーが DVD ドライブ 61 に対して送出され（ステップ S33）、DVD ドライブ 61 がバスデクリプタ 65 によってセッションキー  $K_s$  で復号したセキュアドディスクキーをライタブルディスクに対してライトする処理（ステップ S34）が相違している。

上述した第 10 図および第 12 図に示す構成または方法を採用すると、一般ユーザが自作した CSS 書き込みソフトウェアを使って作成した CSS 暗号化データイメージを、通常のライトコマンドで書き込むことが可能という欠陥がある。理由は、CSS 方式のアルゴリズムは秘密とは言えず、公知とされていることによる。第 10 図の例であれば、認証が成立した時点でアプリケーションソフトウェアを自作のものに切り替え、また、ライタブルディスク 13 a に予め記録されたセキュアドディスクキーに合わせて、自ら生成したタイトルキーを利用してコンテンツをスクランブルする CSS スクランブラを CSS 契約を受けない者が作成することが可能である。

次に、さらなる構成例について説明する。上述した第 10 図および第 12 図に示す構成または方法では、スクランブルド MPEG データが DVD ドライブ 61 と PC 71 間の ATAPI 等の標準化されたインターフェースを通るために、書き込み中のスクランブルド MPEG データが横から盗まれ、これに「DeCSS」を施すことで平文に戻すという行



為がなされる危険性がある。この点を考慮してスクランブルドMPEGデータに対してもバス暗号化および復号を施すものが第14図および第16図にそれぞれ示す構成例である。

第14図の構成例は、予めライタブルディスク13a上にセキュアド  
5 ディスクキー10aが記録されている点は、第10図のシステムと同様である。第10図のシステムと相違する点は、スクランブラ53の出力に得られるスクランブルドMPEGデータがバスエンクリプタ76によって暗号化されてからDVDドライブ61にインターフェースを介して伝送され、DVDドライブ61において、バスデクリプタ66によって  
10 復号されることである。これによって、インターフェースを通る時にスクランブルドMPEGデータが横取りされるおそれを少なくできる。

第15図は、第14図のシステムにおけるDVDドライブ61とPC  
71との間の信号の授受の手順を示す。この手順は、第10図のシステムの手順を示す第11図と同様のものである。相違する点は、ステップ  
15 S28において、スクランブルドMPEGデータを送る処理がステップS38のセッションキーKsで暗号化されたスクランブルドMPEGデータを送ることに変わっていることである。

第16図の構成例は、ライタブルディスク13b上にセキュアドディスクキー10bを記録する点は、第12図のシステムと同様である。第  
20 12図のシステムと相違する点は、スクランブラ53の出力に得られるスクランブルドMPEGデータがバスエンクリプタ76によって暗号化されてからDVDドライブ61に伝送され、DVDドライブ61において、バスデクリプタ66によって復号されることである。これによって、インターフェースを通る時にスクランブルドMPEGデータが横取りさ  
25 れるおそれを少なくできる。例えば放送コンテンツから得られたスクランブルドMPEGデータを横取りしてハードディスクに記録し、その後

「D e C S S」でもって復号することがされるおそれがある。

第 1 7 図は、第 1 6 図のシステムにおけるDVDドライブ 6 1 と P C 7 1 との間の信号の授受の手順を示す。この手順は、第 1 2 図のシステムの手順を示す第 1 3 図と同様のものである。相違する点は、ステップ 5 S 2 8 において、スクランブルドMPEGデータを送る処理がステップ S 3 8 のセッションキーK s で暗号化されたスクランブルドMPEGデータを送ることに変わっていることである。

上述した第 1 4 図および第 1 6 図に示すさらなる構成または方法においても、一般ユーザが自作したCSS書き込みソフトウェアを使って作成したCSS暗号化データイメージを、通常のライトコマンドで書き込むことが可能という欠陥がある。

このように、ライタブルディスクに対する書き込みにCSSを適用する場合に生じる問題を、この発明は、解決することができる。以下、図面を参照してこの発明のいくつかの実施形態について説明する。

15 第 1 8 図は、この発明の第 1 の実施形態のシステム構成例を示す。参照符号 1 6 1 がDVDドライブを示し、参照符号 1 7 1 がDVDドライブ 1 6 1 と標準的なインターフェースで接続され、ホストとして機能する情報処理装置例えばP C である。P C 1 7 1 に対してアプリケーションソフトウェアがインストールされ、またはハードウェア（基板）が備  
20 えられることによって、P C 1 7 1 がDVDビデオエンコーダとして機能する。例えばテレビジョンチューナの基板に対してハードウェアのビデオエンコーダ基板が組み込まれる構成とされる。第 1 の実施形態では、予めリードインエリアにセキュアドディスクキー 1 0 a が記録されているライタブルディスク 1 3 a が使用される。例えばライタブルディスク  
25 としては、DVD+R/RW、またはDVD-R/RWを使用できる。

DVDドライブ 1 6 1 は、タイトルキーを生成する乱数発生器 8 1 と、

生成したタイトルキーをディスクキーで暗号化するエンクリプタ 8 2 と、マスターキー 8 3 と、セキュアドディスクキーをマスターキーで復号するデクリプタ 8 4 とを内部に備えている。さらに、認証部 6 2、セッションキー K s でセキュアドディスクキーを暗号化するバスエンクリプタ 6 3、スクランブルド M P E G データを復号するバスデクリプタ 6 6 が備えられている。かかる DVD ドライブ 1 6 1 は、C S S 鍵発行センターの正規の承認を得てこれらの構成要素を備えたものである。また、DVD ドライブ 1 6 1 は、ハードウェア (L S I) で構成されているので、信号処理の内容を外部から知ることが不可能な耐タンパー性を有している。

ライタブルディスク 1 3 a から読まれたセキュアドディスクキー 1 0 a がデクリプタ 8 4 においてマスターキー 8 3 によって復号され、ディスクキーがエンクリプタ 8 2 に供給される。エンクリプタ 8 2 において、乱数発生器 8 1 からのタイトルキーが暗号化され、暗号化タイトルキーが生成される。暗号化タイトルキーが C S S 方式で規定されているようにライタブルディスク 1 3 a に対して記録される。

アプリケーションソフトウェアまたはハードウェア (基板) によって DVD ビデオエンコーダとしての機能を P C 1 7 1 が有する。DVD ドライブ 1 6 1 の認証部 6 2 および P C 1 7 1 の認証部 7 2 の相互認証が成立すると、セッションキー K s が生成される。DVD ドライブ 1 6 1 のバスエンクリプタ 6 3 において、セッションキー K s によってセキュアドディスクキーが暗号化され、バスエンクリプタ 8 5 において、セッションキー K s によって暗号化タイトルキーが暗号化される。これらの暗号化されたデータが標準的インターフェースを介して P C 1 7 1 に伝送される。

P C 1 7 1 では、バスデクリプタ 7 3 において、セッションキー K s

によってセキュアドディスクキーが復号され、バスデクリプタ 7 7 において、セッションキー K s によって暗号化タイトルキーが復号される。デクリプタ 5 6 において、マスターキー 5 7 によってディスクキーが復号され、デクリプタ 7 8 において、バスデクリプタ 7 7 からの暗号化タイトルキーがディスクキーによって復号され、タイトルキーが得られる。

オーディオ／ビジュアルデータ 6 0 が M P E G エンコーダ 5 2 において、M P E G 2 によって圧縮符号化されると共に、D V D 規格のフォーマットのデータへ変換される。例えば M P E G エンコーダ 5 2 では、デジタル放送等で受信されたトランスポートストリームがプログラムストリームへ変換され、D V D フォーマットのデータへ変換される。M P E G エンコーダ 5 2 の出力データがスクランブラ 5 3 にてタイトルキーによってスクランブルされる。スクランブラ 5 3 からのスクランブルド M P E G データがバスエンクリプタ 7 6 において、セッションキー K s によって暗号化される。バスエンクリプタ 7 6 の出力データがインターフェースを介して D V D ドライブ 1 6 1 に伝送される。D V D ドライブ 1 6 1 では、バスデクリプタ 6 6 によってスクランブルド M P E G データが復号され、スクランブルド M P E G データがライタブルディスク 1 3 a に記録される。なお、P C 1 7 1 において、M P E G エンコーダ 5 2 以外の構成要素は、C S S 鍵発行センターの正規の承認を得て備えたものである。

第 1 9 図は、第 1 8 図に示すシステムにおいて、D V D ドライブ 1 6 1 と P C 1 7 1 との間の信号の授受の手順を示す。P C 1 7 1 が D V D ドライブ 1 6 1 に対してコマンドを送り、D V D ドライブ 1 6 1 がコマンドに応答した動作を行う。ライタブルディスクの挿入等でシーケンスが開始し、最初に認証シーケンス A K E (ステップ S 4 1) がなされる。認証が成立すると、セッションキー K s を D V D ドライブ 1 6 1 と P C

1 7 1 が共有する。認証が成立しなかった場合では、処理が中断する。

次に、P C 1 7 1 からの要求に応じてD V Dドライブ1 6 1 がライタブルディスク1 3 a 上のコントロールデータゾーンをシークし、コントロールデータを読み出す（ステップS 4 2）。次のステップS 4 3 において、P C 1 7 1 がセキュアドディスクキーを要求し、D V Dドライブ1 6 1 がセキュアドディスクキーをリードする（ステップS 4 4 およびS 4 5）。D V Dドライブ1 6 1 がバスエンクリプタ6 3 によってセッションキーK s でセキュアドディスクキーを暗号化し、暗号化されたセキュアドディスクキーをD V Dドライブ1 6 1 がP C 1 7 1 に送る（ステップS 4 6）。P C 1 7 1 のバスデクリプタ7 3 がセッションキーK s によってセキュアドディスクキーを復号し、さらに、デクリプタ5 6 によってディスクキーを復号する。

次に、ステップS 4 7 において、認証シーケンスA K E がなされる。認証が成立すると、セッションキーK s が新たに生成され、このセッションキーK s をD V Dドライブ1 6 1 とP C 1 7 1 が共有する。認証が成立しなかった場合では、処理が中断する。認証が成立すると、ステップS 4 8 において、P C 1 7 1 がC G M S をD V Dドライブ1 6 1 に対して送る。ステップS 4 9 において、P C 1 7 1 がD V Dドライブ1 6 1 に対してセッションキーK s で暗号化されたタイトルキーを要求する。D V Dドライブ1 6 1 は、エンクリプタ8 2 からの暗号化タイトルキーをエンクリプタ8 5 に供給し、セッションキーK s で暗号化タイトルキーを暗号化する。このエンクリプタ8 5 からのK s で暗号化された暗号化タイトルキーをP C 1 7 1 に対して戻す（ステップS 5 0）。

P C 1 7 1 では、バスデクリプタ7 7 および7 8 による復号処理によってタイトルキーを生成し、スクランブラ5 3 において、M P E G データを暗号化し、スクランブルドM P E G データを生成する。さらに、ス

クランブルドMPEGデータをバスエンクリプタ76においてセッションキーK<sub>s</sub>で暗号化し、K<sub>s</sub>で暗号化されたスクランブルドMPEGデータをDVDドライブ161に伝送する（ステップS51）。DVDドライブ161は、バスデクリプタ66においてセッションキーK<sub>s</sub>で受け取ったデータを復号してスクランブルドMPEGデータを得る。そして、スクランブルドMPEGデータと暗号化タイトルキーをライタブルディスク13a上にライトする（ステップS52）。

上述した第1の実施形態は、ドライブ161内で生成したタイトルキーをセキュアにPC171へ転送してPC側でのCSSスクランブルに利用し、PC171から受け取ったCSSスクランブルMPEGデータとドライブ161で生成したタイトルキーをライタブルディスク13aへ書き込む方法である。したがって、第1の実施形態は、PC側でタイトルキーを改ざんさせないと同時に、勝手に作成されたタイトルキーでCSSスクランブルをさせないことができ、ライセンスを受けないものが自由にCSSスクランブル書き込みソフトウェアを作ること防止することができる。

第20図は、この発明の第2の実施形態のシステム構成を示す。第2の実施形態は、ライタブルディスク13bに対してセキュアドディスクキーを記録するものである。DVDドライブ161は、タイトルキー生成用の乱数発生器81に加えて、ディスクキー生成用の乱数発生器86が設けられている。ディスクキーがタイトルキーをエンクリプタ82において暗号化するために使用される。また、ディスクキーがマスターキー83によってエンクリプタ87で暗号化され、セキュアドディスクキーが生成される。セキュアドディスクキー10bがライタブルディスク13b上のリードインエリアに記録される。

このように、ディスクキーを生成し、生成したディスクキーを暗号化

してセキュアドディスクキーを生成し、セキュアドディスクキー10bをリードインエリアに記録することを除くと、第2の実施形態の構成および処理は、第18図に示す第1の実施形態のものと同様である。

第21図は、第20図に示すシステムにおいて、DVDドライブ161とPC171との間の信号の授受の手順を示す。第21図に示されるものは、第19図に示す信号の授受の手順と同様である。相違する点は、セキュアドディスクキーをPC171が要求した時に、DVDドライブ161がセキュアドディスクキーをライタブルディスク13bに記録するステップS54と、このセキュアドディスクキーをセッションキーKsで暗号化してPC171に戻す点である。

第2の実施形態は、ドライブ161内で生成したディスクキーとタイトルキーをセキュアにPC171へ転送してPC側ビデオエンコーダーでのCSSスクランブルに利用し、PC171から受け取ったスクランブルDMPEGデータと、ドライブ161で生成したセキュアドディスクキーと、暗号化タイトルキーをライタブルディスクへ書き込む方法である。かかる第2の実施形態は、PC側でタイトルキーを改ざんさせないと同時に、勝手に作成されたタイトルキーでCSSスクランブルをさせないことから、ライセンスを受けないものが自由にCSSスクランブル書き込みソフトウェアを作ること防止する効果がある。さらに、DVDメディアへ予めディスクキーを記録しておく必要がないことから、メディアの製造コストを低くすることができる。

第22図を参照して第3の実施形態について説明する。第3の実施形態では、ライタブルディスク13aのリードインエリアに予めセキュアドディスクキーが記録されている。セキュアドディスクキー10aは、マスターキー83によってデクリプタ84において復号され、ディスクキーが得られる。タイトルキーは、DVDドライブ261内の乱数発生

号化される。エンクリプタ 8 2 からの暗号化タイトルキー 1 1 がライタブルディスク 1 3 a 上に記録される。

DVD ドライブ 2 6 1 は、認証部 9 1 を有し、PC 2 7 1 の認証部 9 2 と相互認証を行う。認証が成立するとセッションキー K s を DVD ドライブ 2 6 1 と PC 2 7 1 とが共有する。この相互認証の方法は、CSS 方式と同様のものに限らず、後述するような新たな方法を採用できる。新たな認証方法を採用することによって、ライセンスを受けないものによる CSS 書き込みソフト作成をより確実に防ぐことが可能となる。

PC 2 7 1 は、認証部 9 2 を有する以外には、オーディオ／ビジュアルデータ 6 0 を符号化する MPEG エンコーダ 5 2 とバスエンクリプタ 9 3 とを有するのみである。その他の処理は、DVD ドライブ 2 6 1 においてなされる。PC 2 7 1 は、CSS スクランブルするための一切の鍵や処理を持たず、相互認証機能を持つのみであり、負荷が著しく軽くなる。

DVD ドライブ 2 6 1 は、PC 2 7 1 からのセッションキー K s で暗号化された MPEG データをバスデクリプタ 9 4 においてセッションキー K s で復号する。そして、スクランブラ 9 5 で暗号化し、スクランブルド MPEG データ 9 をライタブルディスク 1 3 a 上に記録する。スクランブラ 9 5 は、乱数発生器 8 1 によって生成されたタイトルキーによって MPEG データを暗号化し、スクランブルド MPEG データを生成する。

第 3 の実施形態も、PC 側でタイトルキーを改ざんさせないと同時に、勝手に作成されたタイトルキーで CSS スクランブルをさせないことから、ライセンスを受けないものが自由に CSS スクランブル書き込みソフトウェアを作ること防止する効果がある。新たな認証方法を導入すれば、ライセンスを受けない者によって書き込みソフトウェアが作成さ



フトウェアを作ること防止する効果がある。新たな認証方法を導入すれば、ライセンスを受けない者によって書き込みソフトウェアが作成されることをより確実に防止できる。さらに、P C側の負荷を軽くすることができる。

- 5 第23図は、第4の実施形態を示す。第3の実施形態と相違する点は、DVDドライブ261の乱数発生器86によってディスクキーを生成し、ディスクキーをエンクリプタ87においてマスターキー83によって暗号化し、セキュアドディスクキー10bをライタブルディスク13bに対して記録することである。第3の実施形態と同様に、P C271が認  
10 証部92と、パスエンクリプタ93と、MPEGエンコーダ52を有する。

- かかる第4の実施形態も上述した第3の実施形態と同様の作用効果を奏するものである。さらに、DVDメディアへ予めディスクキーを記録しておく必要がないことから、メディアの製造コストを低くすることが  
15 できる。

- 第24図は、第18図に示す第1の実施形態の構成に対して暗号化タイトルキーのマスク制御機構としてのマスクコントロール101を加えた第5の実施形態を示す。マスクコントロール101に対してエンクリプタ82からの暗号化タイトルキーが入力され、マスクコントロール1  
20 01の出力に取り出された暗号化タイトルキー11がライタブルディスク13a上に記録される。

- マスクコントロール101は、DVDドライブ161の認証部62の認証の結果に応答してマスク機能が制御される。すなわち、P C171とDVDドライブ161の相互認証が成立し、セッションキーKsが生成  
25 成されている間はマスク機能が解除され、暗号化タイトルキー11がライタブルディスク13a上に記録される。一方、認証が成立しなければ

マスク機能は有効となり、暗号化タイトルキー 1 1 が無効データまたはダミーデータ例えばゼロデータに置き換えられ、暗号化タイトルキーのライタブルディスク 1 3 a 上への書き込みが実質的に禁止される。

第 2 5 図は、第 2 0 図に示す第 2 の実施形態の構成に対して暗号化タイトルキーのマスク制御機構としてのマスクコントロール 1 0 1 と、セキュアドディスクキーのマスク制御機構としてのマスクコントロール 1 0 2 とを加えた第 6 の実施形態を示す。マスクコントロール 1 0 1 と同様に、マスクコントロール 1 0 2 は、セキュアドディスクキーに対してマスク機能を発揮する。すなわち、P C 1 7 1 と D V D ドライブ 1 6 1 の相互認証が成立し、セッションキー K s が生成されている間はマスク機能が解除され、セキュアドディスクキー 1 0 b がライタブルディスク 1 3 b 上に記録される。一方、認証が成立しなければマスク機能は有効となり、セキュアドディスクキー 1 0 b がライタブルディスク 1 3 b 上に記録されない。

上述した第 5 および第 6 の実施形態のように、ディスクへの C S S キーの書き込みを相互認証の成立結果によって制御することによって、一般のユーザによる C S S 書き込みソフトウェアの作成をより確実に禁止することが可能となる。それによって正規に許可された者だけが C S S 書き込みアプリケーションソフトウェアを作成することができる。

第 2 6 図は、第 2 2 図に示す第 3 の実施形態の構成に対して暗号化タイトルキーのマスク制御機構としてのマスクコントロール 1 0 3 を加えた第 7 の実施形態を示す。マスクコントロール 1 0 3 に対してエンクリプタ 8 2 からの暗号化タイトルキーが入力され、マスクコントロール 1 0 3 の出力に取り出された暗号化タイトルキー 1 1 がライタブルディスク 1 3 a 上に記録される。

マスクコントロール 1 0 3 は、D V D ドライブ 1 6 1 の認証部 6 2 の

認証の結果に応答してマスク機能が制御される。すなわち、P C 1 7 1  
とD V Dドライブ1 6 1の相互認証が成立し、セッションキーK sが生  
成されている間はマスク機能が解除され、暗号化タイトルキー1 1がラ  
イタブルディスク1 3 a上に記録される。一方、認証が成立しなければ  
5 マスク機能は有効となり、暗号化タイトルキー1 1がライタブルディス  
ク1 3 a上に記録されない。

第2 7図は、第2 3図に示す第4の実施形態の構成に対して暗号化タ  
イトルキーのマスク制御機構としてのマスクコントロール1 0 3と、セ  
キュアドディスクキーのマスク制御機構としてのマスクコントロール1  
10 0 4とを加えた第8の実施形態を示す。マスクコントロール1 0 3と同  
様に、マスクコントロール1 0 4は、セキュアドディスクキーに対して  
マスク機能を発揮する。すなわち、P C 1 7 1とD V Dドライブ1 6 1  
の相互認証が成立し、セッションキーK sが生成されている間はマスク  
機能が解除され、セキュアドディスクキー1 0 bがライタブルディスク  
15 1 3 b上に記録される。一方、認証が成立しなければマスク機能は有効  
となり、セキュアドディスクキー1 0 bがライタブルディスク1 3 b上  
に記録されない。

上述した第7および第8の実施形態のように、ディスクへのC S Sキ  
ーの書き込みを相互認証の成立結果によって制御することによって、一  
20 般のユーザによるC S S書き込みソフトウェアの作成をより確実に禁止  
することが可能となる。それによって正規に許可された者だけがC S S  
書き込みアプリケーションソフトウェアを作成することができる。

第2 8図は、上述した第3の実施形態（第2 2図）、第4の実施形態  
（第2 3図）、第7の実施形態（第2 6図）および第8の実施形態（第  
25 2 7図）のそれぞれに備えられている認証部9 1および9 2に適用され  
る認証構成または方法の一例を説明するものである。第2 8図に示す例

では、相互認証からセッションキーを生成すると同時に、ディスクタイプの情報をセキュアにドライブからPCへ伝えるようにしている。ディスクタイプデータは、下記のように定義された2ビットの情報である。

(0, 0) : ROM      (0, 1) : 未定義      (1, 0) : ライタブルタイプ1  
5      (1, 1) : ライタブルディスクタイプ2

例えばタイプ1は、リライタブルディスクを示し、タイプ2は、1回のみ記録可能なディスクを示す。他の例としては、タイプ1がCSS方式の書き込みが許されている種類のディスクを意味し、タイプ2がCSS方式の書き込みが許されていない種類のディスクを意味する。ディスクタイプは、ディスク上のリードインエリア内の所定位置に記録されている。但し、ウォブリンググループの情報に記録されているものであっても良く、また、ディスクの光学的特性から判定されたものでも良い。第28図において、参照符号301がディスクタイプデータを示す。

ディスクタイプデータ301がマルチプレクサ302および303に  
15      それぞれ供給され、乱数発生器304および305からの乱数と混合され、ディスクタイプデータを含む64ビットの乱数データRa1およびRa2がそれぞれ生成される。例えば64ビットの乱数中の所定の2ビットのビット位置例えば下位側の2ビットにディスクタイプデータが配置される。この乱数Ra1およびRa2がPC側に伝送され、デマルチプレクサ  
20      401によって乱数Ra1からディスクタイプデータ301をPCが得ることができる。PCは、取得したディスクタイプのデータに対応するアプリケーションソフトウェアを実行する。

DVDドライブ161の認証部91は、認証キーKmを有する。認証キーKmは、多くの場合にLSI内部に配置され、外部から読み出すことができないようセキュアに記憶される。ドライブ161がCSSによる記録を扱う正当なドライブとなるためには、認証キーKmのような著  
25

作権保護技術に関する秘密情報を必要とするので、正規のライセンスを受けずに正規品になりすますようなクローン・ドライブの作成が防止される。

参照符号 306、307 および 308 は、認証キー  $K_m$  をパラメータとして MAC 値を計算する MAC (Message Authentication Code) 演算ブロックをそれぞれ示す。また、参照符号 304、305 および 309 が 64 ビットの乱数を発生する乱数発生器である。上述したように、ディスクタイプと乱数とがマルチプレクサ 302 で合成されてマルチプレクサ 302 から乱数  $R_{a1}$  が出力され、この乱数  $R_{a1}$  が MAC 演算ブロック 306 に供給される。マルチプレクサ 303 からの乱数  $R_{a2}$  が MAC 演算ブロック 307 に供給される。さらに、乱数発生器 309 が乱数  $R_{a3}$  を生成する。乱数発生器 304、305、309 は、例えば LSI の構成の乱数発生器であり、ソフトウェアにより乱数を発生する方法と比較してより真正乱数に近い乱数を発生することができる。乱数発生器を  
15 共通のハードウェアとしても良いが、乱数  $R_{a1}$ 、 $R_{a2}$ 、 $R_{a3}$  は、互いに独立したものである。

PC 側の認証部 92 も、認証キー  $K_m$  を有し、認証キー  $K_m$  をパラメータとして MAC 値を計算する MAC 演算ブロック 406、407 および 408 を備えている。さらに、それぞれ 64 ビットの乱数  $R_{b1}$ 、 $R_{b2}$ 、 $R_{b3}$  をそれぞれ発生する乱数発生器 404、405 および 409 が備え  
20 られている。乱数  $R_{b1}$ 、 $R_{b2}$ 、 $R_{b3}$  は、PC 側の認証部 92 の MAC 演算ブロック 406、407 および 408 にそれぞれ供給されると共に、DVD ドライブ側に伝送され、MAC 演算ブロック 306、307、308 に対して供給される。乱数発生器 404、405、409 は、通常はソフトウェアによって乱数を発生するものであるが、ハードウェア  
25 による乱数が利用できる場合にはこれを用いても良い。

DVDドライブの認証部91において生成された乱数と、PCの認証部92において生成された乱数とが交換される。すなわち、乱数Ra1および乱数Rb1がMAC演算ブロック306および406に入力され、乱数Ra2および乱数Rb2がMAC演算ブロック307および407に入力され、乱数Ra3および乱数Rb3がMAC演算ブロック308および408に入力される。

MAC演算ブロック306が演算したMAC値と、MAC演算ブロック406が演算したMAC値とが認証部92内の比較410において比較され、二つの値が同一か否かが判定される。ここでのMAC値は、 $eK_m(Ra1 \parallel Rb1)$ と表記される。 $eK_m()$ は、認証キーKmを鍵として括弧内のデータを暗号化することを表している。Ra1∥Rb1の記号は、左側に乱数Ra1を配し、右側に乱数Rb1を配するように、二つの乱数を結合することを表している。比較の結果、二つの値が同一と判定されると、PCによるDVDドライブの認証が成功したことになり、そうでない場合には、この認証が失敗したことになる。

MAC演算ブロック307が演算したMAC値と、MAC演算ブロック407が演算したMAC値とがドライブの認証部91内の比較310において比較され、二つの値が同一か否かが判定される。ここでのMAC値は、 $eK_m(Rb2 \parallel Ra2)$ と表記される。比較の結果、二つの値が同一と判定されると、DVDドライブによるPCの認証が成功したことになり、そうでない場合には、この認証が失敗したことになる。

かかる相互認証において、比較310および410の両者において、MAC値が同一と判定され、DVDドライブおよびPCの両者の正当性が確認されると、すなわち、相互認証が成功すると、MAC演算ブロック308および408によって、共通のセッションキー $eK_m(Ra3 \parallel Rb3)$ がそれぞれ生成される。このように、互いのMAC計算値を交換して一

の認証のみを行うようにしても良い。

ディスクタイプデータの他の例を下記に示す。

(0, 0) : ROM      (0, 1) : 未定義 (通常書き込み可能)

(1, 0) : 未定義 (通常書き込み可能)      (1, 1) : ビデ

- 5    オライタブルディスク (CSS/CPRMによるビデオ記録が可能で、私的録画補償金がディスク販売価格に含まれているディスク)

このように定義されたディスクタイプデータが上述したようにPC側に伝送される乱数に混合した場合に、ドライブ側の処理およびPC側の処理の一例を説明する。第29図は、ドライブ側の処理を示すフローチャートである。

- 10    ャートである。

冒頭に挙げた非特許文献3に記載されているように、ディスク上には、ウォブリングしたグループが予め形成されている。ウォブリングは、ADIP (Address in Pre-groove) と称される情報によって変調されたものである。ADIPに含まれる情報の一つがメディアタイプ (3 バイ

- 15    ト) である。最初のステップST101において、メディアタイプが判別される。判別結果がROMか否かがステップST102において判定される。ROMであれば、ステップST103において、ディスクタイプがROM (0, 0) と判定される。ROMでない場合には、ステップST104において、ディスクアプリケーションコードがビデオライタブルか否かが判定される。

- 20    ADIPに含まれる情報の他のものがディスクアプリケーションコード (1 バイト) である。ディスクアプリケーションコードは、特別のアプリケーションにのみ使用されるように制限されたディスクであるか否かを識別するのに使用される。例えばディスクアプリケーションコード
- 25    によって、ビデオ信号を書き込むことが可能なこと (ビデオライタブル) が識別される。

によって、ビデオ信号を書き込むことが可能なこと（ビデオライタブル）が識別される。

5       ステップST104において、ディスクアプリケーションコードがビデオライタブルであれば、ディスクタイプがビデオライタブルと判定される（ステップST106）。若し、ステップST104において、ディスクアプリケーションコードがビデオライタブルでないと判定されると、ディスクタイプがリザーブド（すなわち、未定義）と判定される（ステップST105）。

10       このようにドライブが判定したディスクタイプが上述したように、相互認証時に交換される乱数に混合されたPC側へ伝送される。第30図は、PC側の処理を示すフローチャートである。ステップST111において、相互認証がなされ、ステップST112において、PCがドライブからディスクタイプデータを取得する。

15       ディスクタイプがROMかどうかステップST113において判定される。ROMと判定されると、ステップST114において、データの書き込みが禁止される。ROMでないと判定されると、ステップST115において、ディスクタイプがビデオライタブルか否かが判定される。ビデオライタブルでないと判定されると、ステップST116において、データ書き込みが可能と判定される。ビデオライタブルであると  
20       判定されると、ステップST117において、CSS/CPRMによる書き込み可能と判定される。

第31図は、認証部91および92の他の例を示す。他の例は、上述した一例が相互認証に加えて、ディスクタイプの情報をDVDドライブからPCへ伝える機能を有するのに対して、CGMSの情報をPCから  
25       DVDに伝えるものである。

PC9の認証部92には、記録しようとするCGMSデータ411が



存在する。CGMSデータ411は、記録すべきビデオデータに含まれる著作権管理情報に基づいた2ビットのデータであり、以下のように定義された2ビットの情報である。

(0, 0) : コピーフリー (0, 1) : EPN (Encryption Plus  
5 Non-assertion) (デジタル放送におけるコンテンツ管理情報) (1,  
0) : 1回のコピーのみ許可 (1, 1) : コピー禁止

CGMSデータ411は、記録しようとするビデオ入力から分離されたものである。例えば分離されたCGMSデータが(1, 0)で1回の  
10 コピーのみ許可されている場合では、ライタブルディスクに記録される  
CGMSデータは、1回コピーがされた結果、(1, 1)のコピー禁止  
に変更される。

PC側の認証部92において、CGMSデータ411がマルチプレク  
サ412および413にそれぞれ供給され、乱数発生器404および4  
05からの乱数と混合され、CGMSデータを含む64ビットの乱数デ  
15 ータRb1およびRb2がそれぞれ生成される。例えば64ビットの乱数中  
の所定の2ビットのビット位置例えば下位側の2ビットにCGMSデー  
タが配置される。この乱数Rb1およびRb2がDVDドライブ側に伝送さ  
れ、デマルチプレクサ311によって乱数Rb2からCGMSデータ41  
1をDVDドライブが得ることができる。CGMSデータ411がライ  
20 タブルディスク上の所定の位置に記録される。

第32図は、MAC演算ブロック306, 307, 308, 406,  
407, 408として、AES (Advanced Encryption Standard)エン  
クリプタを使用した場合の構成例を示す。二つの乱数AおよびBを結合  
した128ビットの乱数A || Bと認証キーKmとがAESエンコーダに  
25 供給され、認証キーKmを鍵として乱数A || Bを暗号化した出力eKm(A  
|| B)が形成される。

さらに、第 28 図に示す構成の場合における相互認証の処理の流れを第 33 図および第 34 図のフローチャートを参照して説明する。第 33 図のフローチャートは、DVD ドライブ側の認証部 91 の処理の流れを示し、第 34 図は、PC 側の認証部 92 の処理の流れを示す。最初に、

5 第 34 図中のステップ ST21 において、コマンド SEND KEY により、認証部 91 に対して乱数発生器 404 および 405 でそれぞれ生成された乱数 Rb1 と乱数 Rb2 が転送される。第 33 図中のステップ ST11 において、認証部 91 が認証部 92 から転送されたこれらの乱数を受け取る。

- 10 その後、認証部 92 は、コマンド REPORT KEY により認証部 91 に対して認証キー Km を鍵とした MAC によるレスポンス値と乱数 Ra1 (ディスクタイプデータを含む) とを認証部 92 へ転送することを要求する (ステップ ST22)。このレスポンス値は、 $eKm(Ra1 \parallel Rb1)$  と表記される。eKm ( ) は、認証キー Km を暗号鍵として括弧内のデータを暗
- 15 号化することを表している。Ra1  $\parallel$  Rb1 の記号は、左側に乱数 Ra1 を配し、右側に乱数 Rb1 を配するように、二つの乱数を結合することを表している。

- 認証部 92 からコマンド REPORT KEY を受け取った認証部 91 は、ステップ ST12 において、MAC 演算ブロック 306 が生成した MAC
- 20 値  $eKm(Ra1 \parallel Rb1)$  と乱数 Ra1 を認証部 92 へ転送する。ステップ ST23 において、認証部 92 は、自身の MAC 演算ブロック 406 で MAC 値を計算し、比較 410 において認証部 91 から受け取った値と一致するかの確認を行う。若し、受け取った MAC 値と計算された MAC 値とが一致すれば、認証部 92 (PC) による認証部 91 (DVD ドライ
- 25 プ) の認証が成功したことになる。ステップ ST23 における比較の結果が同一でない場合には、認証部 92 (PC) による認証部 91 (DV

Dドライブ)の認証が失敗したことになり、リジェクト処理がなされる。

認証部92による認証部91の認証が成功した場合には、ステップS  
T24において、認証部92が認証部91へコマンドREPORT KEYを送  
付し、認証部91から乱数Ra2(ディスクタイプデータを含む)と乱数  
5 Ra3の転送を要求する。このコマンドに応答して、ステップST13に  
おいて、認証部91は、これらの乱数を認証部92へ転送する。

ステップST25において、認証部92のMAC演算ブロック407  
は、認証部91から受け取った乱数から認証部92が持つ認証キーKm  
を鍵としたMACによるレスポンス値eKm(Rb2 || Ra2)を計算し、乱数Rb  
10 3とともに、コマンドSEND KEYを用いて認証部91へ転送する。

ステップST14において、認証部91は、認証部92からレスポ  
ンス値eKm(Rb2 || Ra2)および乱数Rb3を受け取ると、自身でMAC値を計算  
し、ステップST15において、比較310によって認証部92から受  
け取ったMAC値と一致するかの確認を行う。若し、受け取ったMAC  
15 値と計算されたMAC値とが一致すれば、認証部91(DVDドライ  
ブ)による認証部92(PC)の認証が成功したことになる。この場合  
には、ステップST16において、MAC演算ブロック308がセッシ  
ョンキーeKm(Ra3 || Rb3)を生成し、また、認証部92に対して認証が成  
功したことを示す情報を送信し、認証処理が完了する。セッションキー  
20 は、認証動作の度に異なる値となる。

ステップST15における比較の結果が同一でない場合には、認証部  
91による認証部92の認証が失敗したことになり、ステップST17  
において、認証が失敗したことを示すエラー情報が認証部92に送信さ  
れる。

25 認証部92は、送付したコマンドSEND KEYに対する応答として認証  
部91から認証が成功したか否かを示す情報を受け取り、受け取った情

報に基づいてステップS T 2 6において、認証完了か否かを判断する。認証が成功したことを示す情報を受け取ることで認証完了と判断し、認証が失敗したことを示す情報を受け取ることで認証が完了しなかったと判断する。認証が完了した場合は、ステップS T 2 7において、M A C  
5 演算ブロック4 0 8がドライブ側と共通のセッションキー $eK_m(Ra3 \parallel Rb3)$ （例えば6 4ビット長）を生成する。認証が完了しなかった場合には、リジェクト処理がなされる。

上述したこの発明の全ての実施形態においては、P CからD V Dドライブへ伝送される記録データをバスエンクリプタで暗号化し、D V Dドライブでは、バスデクリプタで復号している。第3 5図において、参照  
10 符号5 0 1がバスエンクリプタを示し、参照符号5 1 1がバスエンクリプタを示す。

P CからD V Dドライブに対しては、2 K B（キロバイト）のセクタデータからなるバックでもってデータが伝送される。バックは、バック  
15 ヘッダによってバックの種類が指定されている。A Vバック検出部5 0 2は、オーディオバック、ビデバックおよびサブピクチャバックを検出し、検出結果に応じて制御信号を出力する。

A Vバック検出部5 0 2からの制御信号によってセクタ5 0 3が制御される。入力データがオーディオバック、ビデバックおよびサブピク  
20 チャバックの場合には、入力データをA Vデータエンクリプタ5 0 4に導き、セッションキーによって暗号化する。但し、バックヘッダは、暗号化されない。また、これらのバック以外の場合では、入力データを暗号化しないで、インターフェースを介してD V Dドライブに伝送する。

バスデクリプタ5 1 1のA Vバック検出部5 1 2において、受け取ったバックの種類をバックヘッダから検出する。セクタ5 1 3がA Vバック  
25 検出部5 1 2からの制御信号で制御される。バックがオーディオパ

ック、ビデオパックおよびサブピクチャパックの場合には、受取データを  
AVデータデクリプタ 514に導き、セッションキーによって復号する。

CSS方式で保護の対象となるのは、オーディオ／ビジュアルデータ  
であるので、コンピュータのファイルデータ等の他の一般的データを暗  
5 号化する必要がない。そのために、AVパックのみを暗号化している。

第36図は、バス暗号化／復号の処理の流れを示す。ステップST3  
1において、パックヘッダ検出部の検出結果からビデオパックか否かが  
判定される。ビデオパックであれば、ステップST32において、デー  
タが暗号化／復号される。ビデオパックでなければ、ステップST33  
10 のオーディオパックか否かの判定ステップに処理が移る。

ステップST33において、オーディオパックと判定されれば、ステ  
ップST32においてデータが暗号化／復号され、そうでないと判定さ  
れれば、ステップST34のサブピクチャパックか否かの判定ステップ  
に処理が移る。ステップST34において、サブピクチャパックと判定  
15 されれば、ステップST32においてデータが暗号化／復号され、そう  
でないと判定されれば、データを暗号化／復号しない（ステップST3  
5）。そして、バス暗号化／復号の処理が終了する。

第37図は、DVDビデオデータのオーディオパック、ビデオパック  
またはサブピクチャパックの構成を示す。パックの制御情報が配置され  
20 たパックヘッダが先頭に配置され、その後にパケットヘッダが配置され、  
その後にオーディオデータ（AC3データ）、ビデオデータ（MP EG  
プログラムストリーム）またはサブピクチャデータ（字幕等のテキスト  
データ）が配置される。パックヘッダおよびパケットヘッダは、可変長  
データであるので、これらのデータ長が最も長い場合を考慮して、パッ  
25 クヘッダおよびパケットヘッダを含む例えば128バイトがバス暗号化  
／復号の対象外とされ、残りの1920バイトがバス暗号化／復号の対

象とされる。合計の 2 K ( 2 0 4 8 ) バイトが 1 セクタのメインデータとされる。

上述した第 5 の実施形態 ( 第 2 4 図 ) 、第 6 の実施形態 ( 第 2 5 図 ) 、第 7 の実施形態 ( 第 2 6 図 ) および第 8 の実施形態 ( 第 2 7 図 ) では、

5 DVDドライブとPCとの相互認証が成立したか否かに応じて制御されるマスクコントロール 1 0 1、1 0 2、1 0 3、1 0 4 を設けている。これらのマスクコントロールのマスクの対象とするデータについて説明する。最初にライタブルディスクに記録されるデータの構成について説明する。

- 10 DVDドライブでは、PCから受け取ったデータをセクタ構造に変換してライタブルディスクに記録する。第 3 8 図は、1 セクタのデータ構成を示す。2 K バイトのメインデータに対して 1 2 バイトのセクタヘッダが付加され、また、最後の 4 バイトがセクタ全体の対するエラー検出コード E D C とされ、全体で 2 0 6 4 バイトのデータセクタが構成されている。
- 15

セクタヘッダの先頭の 4 バイトがセクタ番号等の I D であり、その後の 2 バイトが I D に対するエラー検出用コード I E D であり、その後の 6 バイトがコピー管理用データ C P R \_ M A I ( Copyright Management Information ) である。C P R \_ M A I は、コピー管理 ( 著作権管理 )

20 が必要なデータがメインデータとして記録される場合に必要データである。C P R \_ M A I 内にメインデータを復号するのに必要な暗号化タイトルキーが配置されている。

- 第 3 8 図に示すセクタ構造のデータを記録時に生成する処理を第 3 9 図を参照して説明する。第 3 9 図に示すように、セクタヘッダの I D が
- 25 用意される。この I D は、DVDドライブ内のCPUによって生成される。すなわち、記録時にPCからライトコマンドがDVDドライブに対

して伝送され、書き込みコマンドにディスクへの記録位置を示すL B A (Logical Block Address)データと、ライトデータ長のデータが付加されている。D V DドライブのC P Uは、ライトコマンドの指示内容が実行可能であると判断すると、ライトデータ長の分だけ、P Cからドライブのバッファメモリに対して2 Kバイトのパック単位でデータを伝送させて蓄える。

そして、実際にライト動作を開始する前に、L B Aデータからディスク上の物理的地址であるP S N (Physical Sector Number)を計算し、その値をI Dとする。そのI Dに対してエラー検出コードI E Dが付加され、I D + I E D (6 バイト) が形成される。

さらに、(I D + I E D) データに対してC P R \_\_M A I およびメインデータが付加され、さらに、これらのデータからセクタ毎のエラー検出符号E D Cが生成され(ステップS T 4 1)、スクランブルされる前の1 単位(1 フレーム)のデータが形成され、その1 単位のデータ内のメインデータに対してタイトルキーでスクランブルが施され、スクランブルドメインデータを含むフレームが形成される(ステップS T 4 2)。

さらに、スクランブルが施されたフレームを1 6 フレーム集めたデータに対してエラー訂正符号化を行う(ステップS T 4 3)。エラー訂正符号化で生成されたE C Cが付加された1 6 フレームのデータ内のメインデータに対してインターリーブ処理が施される(ステップS T 4 4)。そして、セクタ毎に2 6 シンクフレームを変調する(ステップS T 4 5)。変調処理後のデータがライタブルディスクに記録される。

第4 0 図は、6 バイトのC P R \_\_M A I のより詳細なデータ構成を示す。第4 0 図Aは、(P S N < 0 3 0 0 0 0 h) のリードインエリア内のC P R \_\_M A I のデータ構成を示し、第4 0 図Bは、(P S N ≥ 0 3 0 0 0 0 h) のデータエリア内のC P R \_\_M A I のデータ構成を示す。

第40図Aに示すリードインエリア内のCPR\_\_MAIは、一種の属性情報であり、書かれているデータがセキュアドディスクキーであることを示す情報が含まれている。先頭の1バイトBP0が著作権保護システムタイプを示す。例えば著作権保護システムタイプがCSS対応か否か、並びにCPRM対応のものか否かが示される。

次のバイトBP1は、セキュアドディスクキーモードである。次のバイトBP2およびBP3は、未定義である。次のバイトBP4の上位の2ビットが未定義とされ、下位の6ビットがビデオ認証コントロールコードとされる。さらに、バイトBP5が地域（リージョン）管理情報とされている。

第40図Aにおいて破線で囲んで示すように、リードインエリア内のCPR\_\_MAIの全てのデータがマスクの対象とされる。すなわち、認証が成立しないでマスクを行う時には、リードインエリア内のCPR\_\_MAIの全てのデータが例えば00hのデータに書き換えられる。ビデオ認証コントロールコードは必ずしもマスクしないでも良い。なお、後述するマスクコントロールのためのCPR\_\_MAIフィルタにおいては、リードインエリア内のCPR\_\_MAIの中で、所定の暗号化方式（例えばCSS方式）であることを示す情報は、先頭のバイトBP0であるので、このバイトBP0を暗号化方式を示す情報以外の情報例えば00hのデータに書き換えることで、実質的にCPR\_\_MAIの全てのデータのマスクを行うようにしている。

第40図Bに示すデータエリア内のCPR\_\_MAIについて説明すると、先頭のバイトBP0にCPM（1ビット）、CP\_\_SEC（1ビット）、CGMS（2ビット）、CPS\_\_MOD（4ビット）が配置されている。そして、残りの5バイトBP1～BP5に対して暗号化ビデオタイトルキーが上位側から下位側に向かって順に配置されている。



第40図Bにおいて破線で囲んで示すように、データエリア内のCPR\_\_MAIの内の先頭バイトBP0以外のバイトBP1-BP5（暗号化ビデオタイトルキー）がマスクの対象とされる。すなわち、認証が成立しないでマスクを行う時には、リードインエリア内のCPR\_\_MAIのバイトBP1-BP5が例えば00hのデータに書き換えられる。

第41図は、リードインエリア内並びにデータエリア内のCPR\_\_MAIに対するマスクコントロールの構成の一例を示す。この例では、第39図に示される記録処理において、EDCを加えるステップST41の直前でマスクコントロールを行うようにしている。第41図において、参照符号601がセクタ情報（1バイト）が蓄えられているレジスタであり、参照符号602がPSN（3バイト）が蓄えられているレジスタである。これらの4バイトのIDが演算部603に入力され、2バイトのエラー検出符号IEDが算出される。

参照符号604は、CPR\_\_MAI（6バイト）が蓄えられているレジスタである。参照符号605は、1セクタのメインデータ（2Kバイト）が蓄えられているバッファメモリである。CPR\_\_MAIがCPR\_\_MAIフィルタ606に入力され、マスクコントロールの処理を受ける。フィルタ606の出力にマスクコントロールされたCPR\_\_MAI、すなわち、RSV（6バイト）が取り出される。

エラー検出符号IED（2バイト）と、RSV（6バイト）と、セクタ情報（1バイト）と、PSN（3バイト）と、メインデータ（2048バイト）とが演算部607に入力され、演算部607によってセクタ全体のエラー検出符号EDCが生成される。参照符号608で示すミキサーに対してセクタ情報、PSN、エラー検出コードIED、RSV、メインデータ、EDCが入力され、第38図に示す構成の1セクタのデータが構成される。

互認証前の段階で、CSSキーの書き込みを禁止するためのマスクを行う場合の構成を示す。なお、第42図、後述する第43図および第44図において、破線が囲んだCPR\_\_MAIフィルタ606は、論理ゲートによって構成されている。ディスク上のアドレスであるPSN（3バイト）が比較器611に入力され、所定のアドレス例えば030000hと比較される。また、CPR\_\_MAIおよび乱数発生器613の生成した乱数がデータ変換器612に供給される。データ変換器612は、比較器611によって制御される。

データ変換器612は、リードインエリアとデータエリアとを指示する比較器611の出力によって、各エリアに応じた処理を行う。比較器611の出力によって、 $(PSN < 030000h)$ と判定される場合は、リードインエリアに記録されるCPR\_\_MAI（第40図A参照）に対するマスクが行われる。マスクを行うために、データ変換器612がBP0を00hのデータへ置き換える。比較器611の出力が $(PSN < 030000h)$ 以外を示す場合では、データエリアに記録されるCPR\_\_MAI（第40図B参照）に対するマスクが行われる。すなわち、BP0以外の5バイトが全て00hのデータに置き換えられる。

第43図は、相互認証が成立してCSS方式の書き込みが許可される場合、すなわち、CSSキーの書き込み禁止の解除時のCPR\_\_MAIフィルタ606の処理を示す。

比較器611の出力によって、 $(PSN < 030000h)$ と判定されるリードインエリアでは、CPR\_\_MAI（第40図A参照）が出力される。また、 $(PSN < 030000h)$ 以外の場合では、CPR\_\_MAI（第40図B参照）が出力される。タイトルキーを生成するために、6バイト長の乱数発生器613が使用され、乱数発生器613が発生した6バイトの内の5バイトがCPR\_\_MAIの5バイト（BP1,

に、6 バイト長の乱数発生器 6 1 3 が使用され、乱数発生器 6 1 3 が発生した 6 バイトの内の 5 バイトが C P R \_ M A I の 5 バイト ( B P 1 , B P 2 , B P 3 , B P 4 , B P 5 ) として用いられる。

第 4 4 図は、マスクコントロールの応用例を示す。応用例は、相互認  
証の成立をトリガーとしてリードインエリアの B P 1 ~ B P 5 を乱数で埋めることを許可する例であり、ディスクキーのマスクコントロールに対して適用することができる。

比較器 6 1 1 の出力によってリードインエリアであることが決定される場合では、B P 0 が 0 0 h とされ、B P 1 ~ B P 5 が乱数発生器 6 1  
4 の出力によって生成された乱数データとされる。この B P 0 ~ B P 5 の 6 バイトがディスクのリードインエリアに記録されるので、そのディスクに固有のユニーク I D が記録される。一方、データエリアでは、タイトルキーを記録する場合と異なり、B P 0 以外の B P 1 ~ B P 5 の 5 バイトが全て 0 0 h とされる。

第 4 5 図は、セッションキーの生成および消滅と、C S S キー ( 暗号化タイトルキーおよびセキュアドディスクキー、または暗号化タイトルキー ) のマスク制御の処理の流れを示すフローチャートである。最初のステップ S T 5 1 では、この発明の対象とする C S S スクランブル書き込みが許可されたディスク例えば D V D + R W / + R ディスクが挿入されたか否かが判定される。ディスクが挿入されたと判定されると、ステップ S T 5 2 において P C アプリケーションが起動されているか否かが判定される。すなわち、P C が電源オン、あるいは再起動を経て、O S が起動し P C からアプリケーションプログラムの実行が可能か否かが判定される。C S S キー書き込みマスク機能は、デフォルトで書き込みを禁止する状態にある。なお、ステップ S T 5 1 および S T 5 2 の順序は、逆であっても良い。

PCアプリケーションが起動されていると、ステップST52で判定されると、ステップST53において、相互認証がなされ、セッションキーが生成される。セッションキーの生成が完了したか否かがステップST54において判定され、若し、完了したと判定されると、CSSキーの書き込みマスク機能が解除される（ステップST55）。

ステップST56において、PCアプリケーションが終了したか否かが判定される。PCアプリケーションが終了したと判定されると、ステップST57において、PC内で生成されたセッションキーが消去される（ステップST57）。そして、PCアプリケーションが再び起動されているかどうか判定される（ステップST58）。起動されていると判定されると、ステップST53に制御が戻る。

ステップST58において、アプリケーションが起動されていないと判定されると、DVD+RW/+Rディスクが排出されたか否かがステップST59において判定される。排出されていないと判定されると、制御がステップST58に戻る。ディスクが排出されたらステップST59において判定されると、ステップST60において、ドライブ内で生成したセッションキーが消去される。そして、マスクコントロールによってCSSキー書き込みが禁止される（ステップST61）。

ステップST56において、アプリケーションが起動されていないと判定されると、DVD+RW/+Rディスクが排出されたか否かがステップST62において判定される。排出されていないと判定されると、制御がステップST56に戻る。ディスクが排出されたらステップST62において判定されると、ステップST63において、ドライブ内で生成したセッションキーが消去される。そして、マスクコントロールによってCSSキー書き込みが禁止される（ステップST61）。

なお、マスターキーの配信構成を特開2002-236622号公報

に記載されているようなツリー構造を使用しても良い。第46図は、第26図に示す実施の形態に対してこの方法を適用した場合の構成を示す。ドライブ261には、複数のドライブで共通のデバイスノードキー111およびドライブ固有のデバイスID112を保持する。また、ライタブルディスク13aには、EKB(Enable Key Block)14と呼ばれるブロックデータによって構成されるテーブルが格納されている。EKBには、複数の暗号化キーが含まれる。

ライタブルディスクからEKBが復号部113に読み込まれ、復号部113において、デバイスノードキー111と、デバイスID112とによってマスターキーが復号される。この方法は、新たなマスターキーの配布、或いはマスターキーの更新に利用することができる。

この発明は、上述したこの発明の一実施形態等に限定されるものではなく、この発明の要旨を逸脱しない範囲内で様々な変形や応用が可能である。例えばマスターキー、ディスクキーおよびタイトルキーの3つの暗号化鍵を使用する暗号化方法であれば、CSS方式以外の暗号化方法を使用しても良い。また、この発明は、ディスク以外に光カード、メモリカード等の媒体に対して情報を記録する場合に対しても適用することができる。

## 請 求 の 範 囲

1. 記録媒体から情報を読み出し、記録媒体に情報を記録する記録再生装置と、上記記録再生装置が伝達手段を介して接続される情報処理装置とを備え、管理機構が管理する第1の暗号化鍵と、記録媒体固有の第2
- 5 の暗号化鍵と、記録の度に生成される第3の暗号化鍵とを使用したコンテンツ情報暗号化方法で暗号化されたコンテンツ情報を記録媒体に記録する信号処理システムであって、
- 上記記録再生装置は、
- 第1の暗号化鍵を保持する保持手段と、
- 10 記録媒体に暗号化されて記録されている第2の暗号化鍵を再生し、上記第1の暗号化鍵で復号する第2の暗号化鍵復号手段と、
- 第3の暗号化鍵を生成する第3の暗号化鍵生成手段と、
- 上記第3の暗号化鍵を復号された第2の暗号化鍵で暗号化する暗号化手段と、
- 15 情報処理装置との間の認証を行い、認証成立時にセッションキーを生成する認証手段と、
- 上記暗号化されて記録されている第2の暗号化鍵を上記セッションキーによってバス暗号化して上記情報処理装置に伝送する第1のバス暗号化手段と、
- 20 暗号化された上記第3の暗号化鍵を上記セッションキーによってバス暗号化して上記情報処理装置に伝送する第2のバス暗号化手段と、
- 上記情報処理装置からの暗号化およびバス暗号化されたコンテンツ情報をバス復号するバス復号手段と、
- 上記暗号化された上記第3の暗号化鍵と、上記暗号化されたコンテンツ
- 25 ツ情報を記録媒体に記録する記録手段とを有し、
- 上記情報処理装置は、

第 1 の暗号化鍵を保持する保持手段と、

上記記録再生装置との間の認証を行い、認証成立時にセッションキーを生成する認証手段と、

- 上記バス暗号化された第 2 の暗号化鍵を上記セッションキーによって
- 5 バス復号して暗号化された上記第 2 の暗号化鍵を復号する第 1 のバス復号手段と、

上記暗号化された第 2 の暗号化鍵を上記第 1 の暗号化鍵で復号する復号手段と、

- 上記バス暗号化された第 3 の暗号化鍵を上記セッションキーによって
- 10 バス復号して上記暗号化された第 3 の暗号化鍵を復号する第 2 のバス復号化手段と、

上記暗号化された第 3 の暗号化鍵を上記第 2 の暗号化鍵で復号する復号手段と、

- 上記記録再生装置に対して伝送するコンテンツ情報を上記第 3 の暗号化で暗号化する暗号化手段と、
- 15

上記暗号化されたコンテンツ情報を上記セッションキーでバス暗号化して上記記録再生装置に送出するバス暗号化手段とを有する信号処理システム。

2. 請求の範囲 1 において、

- 20 上記記録再生装置の上記認証手段と上記情報処理装置の上記認証手段とは、生成した乱数データを交換する時に、上記記録再生装置から上記情報処理装置に伝送する乱数に上記記録媒体の種類の情報を混合するようにした信号処理システム。

3. 請求の範囲 1 において、

- 25 上記記録再生装置の上記認証手段と上記情報処理装置の上記認証手段とは、生成した乱数データを交換する時に、上記情報処理装置から上記

記録再生装置に伝送する乱数に著作権関連情報を混合するようにした信号処理システム。

4. 請求の範囲 1 において、

さらに、暗号化された上記第 3 の暗号化鍵に対するマスク制御手段を  
5 有し、

上記認証手段によって認証が成立している期間のみ、暗号化された上記第 3 の暗号化鍵の上記記録媒体に対する書き込みが可能とされた信号処理システム。

5. 記録媒体から情報を読み出し、記録媒体に情報を記録する記録再生  
10 装置と、上記記録再生装置が伝達手段を介して接続される情報処理装置とを備え、管理機構が管理する第 1 の暗号化鍵と、記録媒体固有の第 2 の暗号化鍵と、記録の度に生成される第 3 の暗号化鍵とを使用したコンテンツ情報暗号化方法で暗号化されたコンテンツ情報を記録媒体に記録する信号処理システムであって、

15 上記記録再生装置は、

第 1 の暗号化鍵を保持する保持手段と、

第 2 の暗号化鍵を生成する第 2 の暗号化鍵生成手段と、

生成された第 2 の暗号化鍵を第 1 の暗号化鍵で暗号化する暗号化手段と、

20 第 3 の暗号化鍵を生成する第 3 の暗号化鍵生成手段と、

生成された第 2 の暗号化鍵で上記第 3 の暗号化鍵を暗号化する暗号化手段と、

情報処理装置との間の認証を行い、認証成立時にセッションキーを生成する認証手段と、

25 上記暗号化された第 2 の暗号化鍵を上記セッションキーによってバス暗号化して上記情報処理装置に伝送する第 1 のバス暗号化手段と、



暗号化された上記第 3 の暗号化鍵を上記セッションキーによってバス暗号化して上記情報処理装置に伝送する第 2 のバス暗号化手段と、

上記情報処理装置からの暗号化およびバス暗号化されたコンテンツ情報をバス復号するバス復号手段と、

- 5      上記暗号化された上記第 2 の暗号化鍵と、上記暗号化された上記第 3 の暗号化鍵と、上記暗号化されたコンテンツ情報を記録媒体に記録する記録手段とを有し、

    上記情報処理装置は、

    第 1 の暗号化鍵を保持する保持手段と、

- 10     上記記録再生装置との間の認証を行い、認証成立時にセッションキーを生成する認証手段と、

    上記バス暗号化された第 2 の暗号化鍵を上記セッションキーによってバス復号して暗号化された上記第 2 の暗号化鍵を復号する第 1 のバス復号手段と、

- 15     上記暗号化された第 2 の暗号化鍵を上記第 1 の暗号化鍵で復号する復号手段と、

    上記バス暗号化された第 3 の暗号化鍵を上記セッションキーによってバス復号して上記暗号化された第 3 の暗号化鍵を復号する第 2 のバス復号化手段と、

- 20     上記暗号化された第 3 の暗号化鍵を上記第 2 の暗号化鍵で復号する復号手段と、

    上記記録再生装置に対して伝送するコンテンツ情報を上記第 3 の暗号化で暗号化する暗号化手段と、

- 上記暗号化されたコンテンツ情報を上記セッションキーでバス暗号化  
25     して上記記録再生装置に送出するバス暗号化手段とを有する信号処理システム。

6. 請求の範囲 5 において、

上記記録再生装置の上記認証手段と上記情報処理装置の上記認証手段とは、生成した乱数データを交換する時に、上記記録再生装置から上記情報処理装置に伝送する乱数に上記記録媒体の種類の情報を混合するよう  
5 にした信号処理システム。

7. 請求の範囲 5 において、

上記記録再生装置の上記認証手段と上記情報処理装置の上記認証手段とは、生成した乱数データを交換する時に、上記情報処理装置から上記記録再生装置に伝送する乱数に著作権関連情報を混合するようにした信  
10 号処理システム。

8. 請求の範囲 5 において、

さらに、暗号化された上記第 3 の暗号化鍵に対する第 1 のマスク制御手段と、暗号化された上記第 2 の暗号化鍵に対する第 2 のマスク制御手段とを有し、

15 上記認証手段によって認証が成立している期間のみ、暗号化された上記第 3 の暗号化鍵および暗号化された上記第 2 の暗号化鍵の上記記録媒体に対する書き込みが可能とされた信号処理システム。

9. 記録媒体から情報を読み出し、記録媒体に情報を記録する記録再生装置と、上記記録再生装置が伝達手段を介して接続される情報処理装置  
20 とを備え、管理機構が管理する第 1 の暗号化鍵と、記録媒体固有の第 2 の暗号化鍵と、記録の度に生成される第 3 の暗号化鍵とを使用したコンテンツ情報暗号化方法で暗号化されたコンテンツ情報を記録媒体に記録する信号処理システムであって、

上記記録再生装置は、

25 第 1 の暗号化鍵を保持する保持手段と、

記録媒体に暗号化されて記録されている第 2 の暗号化鍵を再生し、上

記第 1 の暗号化鍵で復号する第 2 の暗号化鍵復号手段と、  
第 3 の暗号化鍵を生成する第 3 の暗号化鍵生成手段と、  
第 3 の暗号化鍵を復号された第 2 の暗号化鍵で暗号化する暗号化手段と、

- 5 情報処理装置との間の認証を行い、認証成立時にセッションキーを生成する認証手段と、

上記情報処理装置からのバス暗号化されたコンテンツ情報をバス復号するバス復号手段と、

- 上記コンテンツ情報を上記第 3 の暗号化鍵によって暗号化する暗号化手段と、  
10 手段と、

上記暗号化された上記第 3 の暗号化鍵と、上記暗号化されたコンテンツ情報を記録媒体に記録する記録手段とを有し、

上記情報処理装置は、

- 上記記録再生装置との間の認証を行い、認証成立時にセッションキーを生成する認証手段と、  
15

上記記録再生装置に対して伝送するコンテンツ情報を上記セッションキーでバス暗号化して上記記録再生装置に送出するバス暗号化手段とを有する信号処理システム。

10. 請求の範囲 9 において、

- 20 上記記録再生装置の上記認証手段と上記情報処理装置の上記認証手段とは、生成した乱数データを交換する時に、上記記録再生装置から上記情報処理装置に伝送する乱数に上記記録媒体の種類の情報を混合するようにした信号処理システム。

11. 請求の範囲 9 において、

- 25 上記記録再生装置の上記認証手段と上記情報処理装置の上記認証手段とは、生成した乱数データを交換する時に、上記情報処理装置から上記

記録再生装置に伝送する乱数に著作権関連情報を混合するようにした信号処理システム。

1 2. 請求の範囲 9 において、

さらに、暗号化された上記第 3 の暗号化鍵に対するマスク制御手段を  
5 有し、

上記認証手段によって認証が成立している期間のみ、暗号化された上記第 3 の暗号化鍵の上記記録媒体に対する書き込みが可能とされた信号処理システム。

1 3. 記録媒体から情報を読み出し、記録媒体に情報を記録する記録再生装置と、上記記録再生装置が伝達手段を介して接続される情報処理装置とを備え、管理機構が管理する第 1 の暗号化鍵と、記録媒体固有の第 2 の暗号化鍵と、記録の度に生成される第 3 の暗号化鍵とを使用したコンテンツ情報暗号化方法で暗号化されたコンテンツ情報を記録媒体に記録する信号処理システムであって、  
10

15 上記記録再生装置は、

第 1 の暗号化鍵を保持する保持手段と、

第 2 の暗号化鍵を生成する第 2 の暗号化鍵生成手段と、

生成された第 2 の暗号化鍵を上記第 1 の暗号化鍵で暗号化する暗号化手段と、

20 第 3 の暗号化鍵を生成する第 3 の暗号化鍵生成手段と、

上記第 3 の暗号化鍵を生成された第 2 の暗号化鍵で暗号化する暗号化手段と、

情報処理装置との間の認証を行い、認証成立時にセッションキーを生成する認証手段と、

25 上記情報処理装置からのバス暗号化されたコンテンツ情報をバス復号するバス復号手段と、

上記コンテンツ情報を上記第 3 の暗号化鍵によって暗号化する暗号化手段と、

- 上記暗号化された上記第 2 の暗号化鍵と、上記暗号化された上記第 3 の暗号化鍵と、上記暗号化されたコンテンツ情報を記録媒体に記録する  
5 記録手段とを有し、

上記情報処理装置は、

上記記録再生装置との間の認証を行い、認証成立時にセッションキーを生成する認証手段と、

- コンテンツ情報を上記セッションキーでバス暗号化して上記記録再生  
10 装置に送出するバス暗号化手段とを有する信号処理システム。

1 4. 請求の範囲 1 3 において、

- 上記記録再生装置の上記認証手段と上記情報処理装置の上記認証手段とは、生成した乱数データを交換する時に、上記記録再生装置から上記情報処理装置に伝送する乱数に上記記録媒体の種類の情報を混合するよ  
15 うにした信号処理システム。

1 5. 請求の範囲 1 3 において、

- 上記記録再生装置の上記認証手段と上記情報処理装置の上記認証手段とは、生成した乱数データを交換する時に、上記情報処理装置から上記記録再生装置に伝送する乱数に著作権関連情報を混合するようにした信  
20 号処理システム。

1 6. 請求の範囲 1 3 において、

さらに、暗号化された上記第 3 の暗号化鍵に対する第 1 のマスク制御手段と、暗号化された上記第 2 の暗号化鍵に対する第 2 のマスク制御手段とを有し、

- 25 上記認証手段によって認証が成立している期間のみ、暗号化された上記第 3 の暗号化鍵および暗号化された上記第 2 の暗号化鍵の上記記録媒

体に対する書き込みが可能とされた信号処理システム。

1 7. 伝達手段を介して情報処理装置と接続され、記録媒体から情報を  
読み出し、記録媒体に情報を記録する記録再生装置であって、管理機構  
が管理する第1の暗号化鍵と、記録媒体固有の第2の暗号化鍵と、記録  
5 の度に生成される第3の暗号化鍵とを使用したコンテンツ情報暗号化方  
法で暗号化されたコンテンツ情報を記録媒体に記録する記録再生装置で  
あって、

第1の暗号化鍵を保持する保持手段と、

記録媒体に暗号化されて記録されている第2の暗号化鍵を再生し、上  
10 記第1の暗号化鍵で復号する第2の暗号化鍵復号手段と、

第3の暗号化鍵を生成する第3の暗号化鍵生成手段と、

上記第3の暗号化鍵を復号された第2の暗号化鍵で暗号化する暗号化  
手段と、

情報処理装置との間の認証を行い、認証成立時にセッションキーを生  
15 成する認証手段と、

上記暗号化されて記録されている第2の暗号化鍵を上記セッションキー  
によってバス暗号化して上記情報処理装置に伝送する第1のバス暗号  
化手段と、

暗号化された上記第3の暗号化鍵を上記セッションキーによってバス  
20 暗号化して上記情報処理装置に伝送する第2のバス暗号化手段と、

上記情報処理装置からの暗号化およびバス暗号化されたコンテンツ情  
報をバス復号するバス復号手段と、

上記暗号化された上記第3の暗号化鍵と、上記暗号化されたコンテン  
ツ情報を記録媒体に記録する記録手段とを有し、

25 上記暗号化およびバス暗号化されたコンテンツ情報は、上記第3の暗  
号化鍵で暗号化され、さらに、暗号化コンテンツ情報を情報処理装置で

生成されたセッションキーでバス暗号化したものである記録再生装置。

18. 請求の範囲17において、

上記認証手段は、生成した乱数データを交換する時に、上記情報処理装置に伝送する乱数に上記記録媒体の種類の情報を混合するようにした  
5 記録再生装置。

19. 請求の範囲17において、

さらに、暗号化された上記第3の暗号化鍵に対するマスク制御手段を有し、

上記認証手段によって認証が成立している期間のみ、暗号化された上  
10 記第3の暗号化鍵の上記記録媒体に対する書き込みが可能とされた記録再生装置。

20. 伝達手段を介して情報処理装置と接続され、記録媒体から情報を読み出し、記録媒体に情報を記録する記録再生装置であって、管理機構が管理する第1の暗号化鍵と、記録媒体固有の第2の暗号化鍵と、記録  
15 の度に生成される第3の暗号化鍵とを使用したコンテンツ情報暗号化方法で暗号化されたコンテンツ情報を記録媒体に記録する記録再生装置であって、

第1の暗号化鍵を保持する保持手段と、

第2の暗号化鍵を生成する第2の暗号化鍵生成手段と、

20 生成された第2の暗号化鍵を第1の暗号化鍵で暗号化する暗号化手段と、

第3の暗号化鍵を生成する第3の暗号化鍵生成手段と、

生成された第2の暗号化鍵で上記第3の暗号化鍵を暗号化する暗号化手段と、

25 情報処理装置との間の認証を行い、認証成立時にセッションキーを生成する認証手段と、

上記暗号化された第 2 の暗号化鍵を上記セッションキーによってバス暗号化して上記情報処理装置に伝送する第 1 のバス暗号化手段と、

暗号化された上記第 3 の暗号化鍵を上記セッションキーによってバス暗号化して上記情報処理装置に伝送する第 2 のバス暗号化手段と、

- 5     上記情報処理装置からの暗号化およびバス暗号化されたコンテンツ情報をバス復号するバス復号手段と、

上記暗号化された上記第 2 の暗号化鍵と、上記暗号化された上記第 3 の暗号化鍵と、上記暗号化されたコンテンツ情報を記録媒体に記録する記録手段とを有し、

- 10     上記暗号化およびバス暗号化されたコンテンツ情報は、上記第 3 の暗号化鍵で暗号化され、さらに、暗号化コンテンツ情報を情報処理装置で生成されたセッションキーでバス暗号化したものである記録再生装置。

2 1. 請求の範囲 2 0 において、

- 15     上記認証手段は、生成した乱数データを交換する時に、上記情報処理装置に伝送する乱数に上記記録媒体の種類の情報を混合するようにした記録再生装置。

2 2. 請求の範囲 2 0 において、

- 20     さらに、暗号化された上記第 3 の暗号化鍵に対する第 1 のマスク制御手段と、暗号化された上記第 2 の暗号化鍵に対する第 2 のマスク制御手段とを有し、

上記認証手段によって認証が成立している期間のみ、暗号化された上記第 3 の暗号化鍵および暗号化された上記第 2 の暗号化鍵の上記記録媒体に対する書き込みが可能とされた記録再生装置。

- 25     2 3. 伝達手段を介して情報処理装置と接続され、記録媒体から情報を読み出し、記録媒体に情報を記録する記録再生装置であって、管理機構が管理する第 1 の暗号化鍵と、記録媒体固有の第 2 の暗号化鍵と、記録



の度に生成される第 3 の暗号化鍵とを使用したコンテンツ情報暗号化方法で暗号化されたコンテンツ情報を記録媒体に記録する記録再生装置であって、

第 1 の暗号化鍵を保持する保持手段と、

- 5     記録媒体に暗号化されて記録されている第 2 の暗号化鍵を再生し、上記第 1 の暗号化鍵で復号する第 2 の暗号化鍵復号手段と、

第 3 の暗号化鍵を生成する第 3 の暗号化鍵生成手段と、

第 3 の暗号化鍵を復号された第 2 の暗号化鍵で暗号化する暗号化手段と、

- 10    情報処理装置との間の認証を行い、認証成立時にセッションキーを生成する認証手段と、

上記情報処理装置からのバス暗号化されたコンテンツ情報をバス復号するバス復号手段と、

- 15    上記コンテンツ情報を上記第 3 の暗号化鍵によって暗号化する暗号化手段と、

上記暗号化された上記第 3 の暗号化鍵と、上記暗号化されたコンテンツ情報を記録媒体に記録する記録手段とを有し、

- 20    上記バス暗号化されたコンテンツ情報は、暗号化コンテンツ情報を情報処理装置で生成されたセッションキーでバス暗号化したものである記録再生装置。

2 4 . 請求の範囲 2 3 において、

上記認証手段は、生成した乱数データを交換する時に、上記情報処理装置に伝送する乱数に上記記録媒体の種類の情報を混合するようにした記録再生装置。

- 25    2 5 . 請求の範囲 2 3 において、

さらに、暗号化された上記第 3 の暗号化鍵に対するマスク制御手段を

有し、

上記認証手段によって認証が成立している期間のみ、暗号化された上記第 3 の暗号化鍵の上記記録媒体に対する書き込みが可能とされた記録再生装置。

- 5    26. 伝達手段を介して情報処理装置と接続され、記録媒体から情報を読み出し、記録媒体に情報を記録する記録再生装置であって、管理機構が管理する第 1 の暗号化鍵と、記録媒体固有の第 2 の暗号化鍵と、記録の度に生成される第 3 の暗号化鍵とを使用したコンテンツ情報暗号化方法で暗号化されたコンテンツ情報を記録媒体に記録する記録再生装置であって、
- 10    第 1 の暗号化鍵を保持する保持手段と、  
第 2 の暗号化鍵を生成する第 2 の暗号化鍵生成手段と、  
生成された第 2 の暗号化鍵を上記第 1 の暗号化鍵で暗号化する暗号化手段と、
- 15    第 3 の暗号化鍵を生成する第 3 の暗号化鍵生成手段と、  
上記第 3 の暗号化鍵を生成された第 2 の暗号化鍵で暗号化する暗号化手段と、  
情報処理装置との間の認証を行い、認証成立時にセッションキーを生成する認証手段と、
- 20    上記情報処理装置からのバス暗号化されたコンテンツ情報をバス復号するバス復号手段と、  
上記コンテンツ情報を上記第 3 の暗号化鍵によって暗号化する暗号化手段と、  
上記暗号化された上記第 2 の暗号化鍵と、上記暗号化された上記第 3
- 25    の暗号化鍵と、上記暗号化されたコンテンツ情報を記録媒体に記録する記録手段とを有し、

上記バス暗号化されたコンテンツ情報は、暗号化コンテンツ情報を情報処理装置で生成されたセッションキーでバス暗号化したものである記録再生装置。

27. 請求の範囲26において、

- 5     上記認証手段は、生成した乱数データを交換する時に、上記情報処理装置に伝送する乱数に上記記録媒体の種類情報を混合するようにした記録再生装置。

28. 請求の範囲26において、

- 10    さらに、暗号化された上記第3の暗号化鍵に対する第1のマスク制御手段と、暗号化された上記第2の暗号化鍵に対する第2のマスク制御手段とを有し、

上記認証手段によって認証が成立している期間のみ、暗号化された上記第3の暗号化鍵および暗号化された上記第2の暗号化鍵の上記記録媒体に対する書き込みが可能とされた記録再生装置。

- 15    29. 記録媒体から情報を読み出し、記録媒体に情報を記録する記録再生装置と、上記記録再生装置が伝達ステップを介して接続される情報処理装置とを備え、管理機構が管理する第1の暗号化鍵と、記録媒体固有の第2の暗号化鍵と、記録の度に生成される第3の暗号化鍵とを使用したコンテンツ情報暗号化方法で暗号化されたコンテンツ情報を記録媒体  
20    に記録する記録方法であって、

上記記録再生装置は、

第1の暗号化鍵を保持する保持ステップと、

記録媒体に暗号化されて記録されている第2の暗号化鍵を再生し、上記第1の暗号化鍵で復号する第2の暗号化鍵復号ステップと、

- 25    第3の暗号化鍵を生成する第3の暗号化鍵生成ステップと、

上記第3の暗号化鍵を復号された第2の暗号化鍵で暗号化する暗号化

ステップと、

情報処理装置との間の認証を行い、認証成立時にセッションキーを生成する認証ステップと、

上記暗号化されて記録されている第2の暗号化鍵を上記セッションキーによってバス暗号化して上記情報処理装置に伝送する第1のバス暗号化ステップと、

暗号化された上記第3の暗号化鍵を上記セッションキーによってバス暗号化して上記情報処理装置に伝送する第2のバス暗号化ステップと、

上記情報処理装置からの暗号化およびバス暗号化されたコンテンツ情報をバス復号するバス復号ステップと、

上記暗号化された上記第3の暗号化鍵と、上記暗号化されたコンテンツ情報を記録媒体に記録する記録ステップとを実行し、

上記情報処理装置は、

第1の暗号化鍵を保持する保持ステップと、

上記記録再生装置との間の認証を行い、認証成立時にセッションキーを生成する認証ステップと、

上記バス暗号化された第2の暗号化鍵を上記セッションキーによってバス復号して暗号化された上記第2の暗号化鍵を復号する第1のバス復号ステップと、

上記暗号化された第2の暗号化鍵を上記第1の暗号化鍵で復号する復号ステップと、

上記バス暗号化された第3の暗号化鍵を上記セッションキーによってバス復号して上記暗号化された第3の暗号化鍵を復号する第2のバス復号化ステップと、

上記暗号化された第3の暗号化鍵を上記第2の暗号化鍵で復号する復号ステップと、

上記記録再生装置に対して伝送するコンテンツ情報を上記第 3 の暗号化で暗号化する暗号化ステップと、

上記暗号化されたコンテンツ情報を上記セッションキーでバス暗号化して上記記録再生装置に送出するバス暗号化ステップとを実行する記録方法。

30. 請求の範囲 29 において、

上記記録再生装置の上記認証ステップと上記情報処理装置の上記認証ステップとは、生成した乱数データを交換する時に、上記記録再生装置から上記情報処理装置に伝送する乱数に上記記録媒体の種類情報を混合するようにした記録方法。

31. 請求の範囲 29 において、

上記記録再生装置の上記認証ステップと上記情報処理装置の上記認証ステップとは、生成した乱数データを交換する時に、上記情報処理装置から上記記録再生装置に伝送する乱数に著作権関連情報を混合するようにした記録方法。

32. 請求の範囲 29 において、

さらに、暗号化された上記第 3 の暗号化鍵に対するマスク制御ステップを有し、

上記認証ステップによって認証が成立している期間のみ、暗号化された上記第 3 の暗号化鍵の上記記録媒体に対する書き込みが可能とされた記録方法。

33. 記録媒体から情報を読み出し、記録媒体に情報を記録する記録再生装置と、上記記録再生装置が伝達ステップを介して接続される情報処理装置とを備え、管理機構が管理する第 1 の暗号化鍵と、記録媒体固有の第 2 の暗号化鍵と、記録の度に生成される第 3 の暗号化鍵とを使用したコンテンツ情報暗号化方法で暗号化されたコンテンツ情報を記録媒体

- に記録する記録方法であって、
- 上記記録再生装置は、
- 第1の暗号化鍵を保持する保持ステップと、
- 第2の暗号化鍵を生成する第2の暗号化鍵生成ステップと、
- 5 生成された第2の暗号化鍵を第1の暗号化鍵で暗号化する暗号化ステップと、
- 第3の暗号化鍵を生成する第3の暗号化鍵生成ステップと、
- 生成された第2の暗号化鍵で上記第3の暗号化鍵を暗号化する暗号化ステップと、
- 10 情報処理装置との間の認証を行い、認証成立時にセッションキーを生成する認証ステップと、
- 上記暗号化された第2の暗号化鍵を上記セッションキーによってバス暗号化して上記情報処理装置に伝送する第1のバス暗号化ステップと、
- 暗号化された上記第3の暗号化鍵を上記セッションキーによってバス
- 15 暗号化して上記情報処理装置に伝送する第2のバス暗号化ステップと、
- 上記情報処理装置からの暗号化およびバス暗号化されたコンテンツ情報をバス復号するバス復号ステップと、
- 上記暗号化された上記第2の暗号化鍵と、上記暗号化された上記第3の暗号化鍵と、上記暗号化されたコンテンツ情報を記録媒体に記録する
- 20 記録ステップとを実行し、
- 上記情報処理装置は、
- 第1の暗号化鍵を保持する保持ステップと、
- 上記記録再生装置との間の認証を行い、認証成立時にセッションキーを生成する認証ステップと、
- 25 上記バス暗号化された第2の暗号化鍵を上記セッションキーによってバス復号して暗号化された上記第2の暗号化鍵を復号する第1のバス復

号ステップと、

上記暗号化された第 2 の暗号化鍵を上記第 1 の暗号化鍵で復号する復号ステップと、

- 上記バス暗号化された第 3 の暗号化鍵を上記セッションキーによって  
5 バス復号して上記暗号化された第 3 の暗号化鍵を復号する第 2 のバス復号化ステップと、

上記暗号化された第 3 の暗号化鍵を上記第 2 の暗号化鍵で復号する復号ステップと、

- 上記記録再生装置に対して伝送するコンテンツ情報を上記第 3 の暗号  
10 化で暗号化する暗号化ステップと、

上記暗号化されたコンテンツ情報を上記セッションキーでバス暗号化して上記記録再生装置に送出するバス暗号化ステップとを実行する記録方法。

3 4. 請求の範囲 3 3 において、

- 15 上記記録再生装置の上記認証ステップと上記情報処理装置の上記認証ステップとは、生成した乱数データを交換する時に、上記記録再生装置から上記情報処理装置に伝送する乱数に上記記録媒体の種類の情報を混合するようにした記録方法。

3 5. 請求の範囲 3 3 において、

- 20 上記記録再生装置の上記認証ステップと上記情報処理装置の上記認証ステップとは、生成した乱数データを交換する時に、上記情報処理装置から上記記録再生装置に伝送する乱数に著作権関連情報を混合するようにした記録方法。

3 6. 請求の範囲 3 3 において、

- 25 さらに、暗号化された上記第 3 の暗号化鍵に対する第 1 のマスク制御ステップと、暗号化された上記第 2 の暗号化鍵に対する第 2 のマスク制

御ステップとを有し、

上記認証ステップによって認証が成立している期間のみ、暗号化された上記第3の暗号化鍵および暗号化された上記第2の暗号化鍵の上記記録媒体に対する書き込みが可能とされた記録方法。

- 5    37. 記録媒体から情報を読み出し、記録媒体に情報を記録する記録再生装置と、上記記録再生装置が伝達ステップを介して接続される情報処理装置とを備え、管理機構が管理する第1の暗号化鍵と、記録媒体固有の第2の暗号化鍵と、記録の度に生成される第3の暗号化鍵とを使用したコンテンツ情報暗号化方法で暗号化されたコンテンツ情報を記録媒体  
10    に記録する記録方法であって、

上記記録再生装置は、

第1の暗号化鍵を保持する保持ステップと、

記録媒体に暗号化されて記録されている第2の暗号化鍵を再生し、上記第1の暗号化鍵で復号する第2の暗号化鍵復号ステップと、

- 15    第3の暗号化鍵を生成する第3の暗号化鍵生成ステップと、

第3の暗号化鍵を復号された第2の暗号化鍵で暗号化する暗号化ステップと、

情報処理装置との間の認証を行い、認証成立時にセッションキーを生成する認証ステップと、

- 20    上記情報処理装置からのバス暗号化されたコンテンツ情報をバス復号するバス復号ステップと、

上記コンテンツ情報を上記第3の暗号化鍵によって暗号化する暗号化ステップと、

- 25    上記暗号化された上記第3の暗号化鍵と、上記暗号化されたコンテンツ情報を記録媒体に記録する記録ステップとを実行し、

上記情報処理装置は、



上記記録再生装置との間の認証を行い、認証成立時にセッションキーを生成する認証ステップと、

上記記録再生装置に対して伝送するコンテンツ情報を上記セッションキーでバス暗号化して上記記録再生装置に送出するバス暗号化ステップ  
5 とを実行する記録方法。

38. 請求の範囲37において、

上記記録再生装置の上記認証ステップと上記情報処理装置の上記認証ステップとは、生成した乱数データを交換する時に、上記記録再生装置から上記情報処理装置に伝送する乱数に上記記録媒体の種類の情報を混合  
10 するようにした記録方法。

39. 請求の範囲37において、

上記記録再生装置の上記認証ステップと上記情報処理装置の上記認証ステップとは、生成した乱数データを交換する時に、上記情報処理装置から上記記録再生装置に伝送する乱数に著作権関連情報を混合するよう  
15 にした記録方法。

40. 請求の範囲37において、

さらに、暗号化された上記第3の暗号化鍵に対するマスク制御ステップを有し、

上記認証ステップによって認証が成立している期間のみ、暗号化された上記第3の暗号化鍵の上記記録媒体に対する書き込みが可能とされた  
20 記録方法。

41. 記録媒体から情報を読み出し、記録媒体に情報を記録する記録再生装置と、上記記録再生装置が伝達ステップを介して接続される情報処理装置とを備え、管理機構が管理する第1の暗号化鍵と、記録媒体固有  
25 の第2の暗号化鍵と、記録の度に生成される第3の暗号化鍵とを使用したコンテンツ情報暗号化方法で暗号化されたコンテンツ情報を記録媒体

に記録する記録方法であって、

上記記録再生装置は、

第 1 の暗号化鍵を保持する保持ステップと、

第 2 の暗号化鍵を生成する第 2 の暗号化鍵生成ステップと、

- 5 生成された第 2 の暗号化鍵を上記第 1 の暗号化鍵で暗号化する暗号化ステップと、

第 3 の暗号化鍵を生成する第 3 の暗号化鍵生成ステップと、

上記第 3 の暗号化鍵を生成された第 2 の暗号化鍵で暗号化する暗号化ステップと、

- 10 情報処理装置との間の認証を行い、認証成立時にセッションキーを生成する認証ステップと、

上記情報処理装置からのバス暗号化されたコンテンツ情報をバス復号するバス復号ステップと、

- 15 上記コンテンツ情報を上記第 3 の暗号化鍵によって暗号化する暗号化ステップと、

上記暗号化された上記第 2 の暗号化鍵と、上記暗号化された上記第 3 の暗号化鍵と、上記暗号化されたコンテンツ情報を記録媒体に記録する記録ステップとを実行し、

上記情報処理装置は、

- 20 上記記録再生装置との間の認証を行い、認証成立時にセッションキーを生成する認証ステップと、

コンテンツ情報を上記セッションキーでバス暗号化して上記記録再生装置に送出するバス暗号化ステップとを実行する記録方法。

4 2. 請求の範囲 4 1 において、

- 25 上記記録再生装置の上記認証ステップと上記情報処理装置の上記認証ステップとは、生成した乱数データを交換する時に、上記記録再生装置

から上記情報処理装置に伝送する乱数に上記記録媒体の種類の情報を混合するようにした記録方法。

4 3. 請求の範囲 4 1 において、

5     上記記録再生装置の上記認証ステップと上記情報処理装置の上記認証ステップとは、生成した乱数データを交換する時に、上記情報処理装置から上記記録再生装置に伝送する乱数に著作権関連情報を混合するようにした記録方法。

4 4. 請求の範囲 4 1 において、

10     さらに、暗号化された上記第 3 の暗号化鍵に対する第 1 のマスク制御ステップと、暗号化された上記第 2 の暗号化鍵に対する第 2 のマスク制御ステップとを有し、

   上記認証ステップによって認証が成立している期間のみ、暗号化された上記第 3 の暗号化鍵および暗号化された上記第 2 の暗号化鍵の上記記録媒体に対する書き込みが可能とされた記録方法。

15     4 5. 記録媒体から情報を読み出し、記録媒体に情報を記録する記録再生装置と、上記記録再生装置が伝達ステップを介して接続される情報処理装置とを備え、管理機構が管理する第 1 の暗号化鍵と、記録媒体固有の第 2 の暗号化鍵と、記録の度に生成される第 3 の暗号化鍵とを使用したコンテンツ情報暗号化方法で暗号化されたコンテンツ情報を記録媒体  
20     に記録する記録方法のプログラムであって、

   上記記録再生装置に、

   第 1 の暗号化鍵を保持する保持ステップと、

   記録媒体に暗号化されて記録されている第 2 の暗号化鍵を再生し、上記第 1 の暗号化鍵で復号する第 2 の暗号化鍵復号ステップと、

25     第 3 の暗号化鍵を生成する第 3 の暗号化鍵生成ステップと、

   上記第 3 の暗号化鍵を復号された第 2 の暗号化鍵で暗号化する暗号化

ステップと、

情報処理装置との間の認証を行い、認証成立時にセッションキーを生成する認証ステップと、

- 5 上記暗号化されて記録されている第2の暗号化鍵を上記セッションキーによってバス暗号化して上記情報処理装置に伝送する第1のバス暗号化ステップと、

暗号化された上記第3の暗号化鍵を上記セッションキーによってバス暗号化して上記情報処理装置に伝送する第2のバス暗号化ステップと、

- 10 上記情報処理装置からの暗号化およびバス暗号化されたコンテンツ情報をバス復号するバス復号ステップと、

上記暗号化された上記第3の暗号化鍵と、上記暗号化されたコンテンツ情報を記録媒体に記録する記録ステップとを実行させ、

上記情報処理装置に、

- 15 第1の暗号化鍵を保持する保持ステップと、

上記記録再生装置との間の認証を行い、認証成立時にセッションキーを生成する認証ステップと、

上記バス暗号化された第2の暗号化鍵を上記セッションキーによってバス復号して暗号化された上記第2の暗号化鍵を復号する第1のバス復

- 20 号ステップと、

上記暗号化された第2の暗号化鍵を上記第1の暗号化鍵で復号する復号ステップと、

上記バス暗号化された第3の暗号化鍵を上記セッションキーによってバス復号して上記暗号化された第3の暗号化鍵を復号する第2のバス復

- 25 号化ステップと、

上記暗号化された第3の暗号化鍵を上記第2の暗号化鍵で復号する復

号ステップと、

上記記録再生装置に対して伝送するコンテンツ情報を上記第 3 の暗号化で暗号化する暗号化ステップと、

上記暗号化されたコンテンツ情報を上記セッションキーでバス暗号化して上記記録再生装置に送出するバス暗号化ステップとを実行させる記録方法のプログラム。

46. 記録媒体から情報を読み出し、記録媒体に情報を記録する記録再生装置と、上記記録再生装置が伝達ステップを介して接続される情報処理装置とを備え、管理機構が管理する第 1 の暗号化鍵と、記録媒体固有の第 2 の暗号化鍵と、記録の度に生成される第 3 の暗号化鍵とを使用したコンテンツ情報暗号化方法で暗号化されたコンテンツ情報を記録媒体に記録する記録方法のプログラムであって、

上記記録再生装置に、

第 1 の暗号化鍵を保持する保持ステップと、

15 第 2 の暗号化鍵を生成する第 2 の暗号化鍵生成ステップと、

生成された第 2 の暗号化鍵を第 1 の暗号化鍵で暗号化する暗号化ステップと、

第 3 の暗号化鍵を生成する第 3 の暗号化鍵生成ステップと、

生成された第 2 の暗号化鍵で上記第 3 の暗号化鍵を暗号化する暗号化ステップと、

情報処理装置との間の認証を行い、認証成立時にセッションキーを生成する認証ステップと、

上記暗号化された第 2 の暗号化鍵を上記セッションキーによってバス暗号化して上記情報処理装置に伝送する第 1 のバス暗号化ステップと、

25 暗号化された上記第 3 の暗号化鍵を上記セッションキーによってバス暗号化して上記情報処理装置に伝送する第 2 のバス暗号化ステップと、

上記情報処理装置からの暗号化およびバス暗号化されたコンテンツ情報をバス復号するバス復号ステップと、

- 上記暗号化された上記第 2 の暗号化鍵と、上記暗号化された上記第 3 の暗号化鍵と、上記暗号化されたコンテンツ情報を記録媒体に記録する
- 5 記録ステップとを実行させ、

上記情報処理装置に、

第 1 の暗号化鍵を保持する保持ステップと、

上記記録再生装置との間の認証を行い、認証成立時にセッションキーを生成する認証ステップと、

- 10 上記バス暗号化された第 2 の暗号化鍵を上記セッションキーによってバス復号して暗号化された上記第 2 の暗号化鍵を復号する第 1 のバス復号ステップと、

上記暗号化された第 2 の暗号化鍵を上記第 1 の暗号化鍵で復号する復号ステップと、

- 15 上記バス暗号化された第 3 の暗号化鍵を上記セッションキーによってバス復号して上記暗号化された第 3 の暗号化鍵を復号する第 2 のバス復号化ステップと、

上記暗号化された第 3 の暗号化鍵を上記第 2 の暗号化鍵で復号する復号ステップと、

- 20 上記記録再生装置に対して伝送するコンテンツ情報を上記第 3 の暗号化で暗号化する暗号化ステップと、

上記暗号化されたコンテンツ情報を上記セッションキーでバス暗号化して上記記録再生装置に送出するバス暗号化ステップとを実行させる記録方法のプログラム。

- 25 47. 記録媒体から情報を読み出し、記録媒体に情報を記録する記録再生装置と、上記記録再生装置が伝達ステップを介して接続される情報処

理装置とを備え、管理機構が管理する第 1 の暗号化鍵と、記録媒体固有の第 2 の暗号化鍵と、記録の度に生成される第 3 の暗号化鍵とを使用したコンテンツ情報暗号化方法で暗号化されたコンテンツ情報を記録媒体に記録する記録方法のプログラムであって、

- 5     上記記録再生装置に、  
      第 1 の暗号化鍵を保持する保持ステップと、  
      記録媒体に暗号化されて記録されている第 2 の暗号化鍵を再生し、上記第 1 の暗号化鍵で復号する第 2 の暗号化鍵復号ステップと、  
      第 3 の暗号化鍵を生成する第 3 の暗号化鍵生成ステップと、
- 10    第 3 の暗号化鍵を復号された第 2 の暗号化鍵で暗号化する暗号化ステップと、  
      情報処理装置との間の認証を行い、認証成立時にセッションキーを生成する認証ステップと、  
      上記情報処理装置からのバス暗号化されたコンテンツ情報をバス復号
- 15    するバス復号ステップと、  
      上記コンテンツ情報を上記第 3 の暗号化鍵によって暗号化する暗号化ステップと、  
      上記暗号化された上記第 3 の暗号化鍵と、上記暗号化されたコンテンツ情報を記録媒体に記録する記録ステップとを実行させ、
- 20    上記情報処理装置に、  
      上記記録再生装置との間の認証を行い、認証成立時にセッションキーを生成する認証ステップと、  
      上記記録再生装置に対して伝送するコンテンツ情報を上記セッションキーでバス暗号化して上記記録再生装置に送出するバス暗号化ステップ
- 25    とを実行させる記録方法のプログラム。

48. 記録媒体から情報を読み出し、記録媒体に情報を記録する記録再

- 生装置と、上記記録再生装置が伝達ステップを介して接続される情報処理装置とを備え、管理機構が管理する第1の暗号化鍵と、記録媒体固有の第2の暗号化鍵と、記録の度に生成される第3の暗号化鍵とを使用したコンテンツ情報暗号化方法で暗号化されたコンテンツ情報を記録媒体
- 5 に記録する記録方法のプログラムであって、
- 上記記録再生装置に、
- 第1の暗号化鍵を保持する保持ステップと、
- 第2の暗号化鍵を生成する第2の暗号化鍵生成ステップと、
- 生成された第2の暗号化鍵を上記第1の暗号化鍵で暗号化する暗号化
- 10 ステップと、
- 第3の暗号化鍵を生成する第3の暗号化鍵生成ステップと、
- 上記第3の暗号化鍵を生成された第2の暗号化鍵で暗号化する暗号化ステップと、
- 情報処理装置との間の認証を行い、認証成立時にセッションキーを生成する認証ステップと、
- 15 上記情報処理装置からのバス暗号化されたコンテンツ情報をバス復号するバス復号ステップと、
- 上記コンテンツ情報を上記第3の暗号化鍵によって暗号化する暗号化ステップと、
- 20 上記暗号化された上記第2の暗号化鍵と、上記暗号化された上記第3の暗号化鍵と、上記暗号化されたコンテンツ情報を記録媒体に記録する記録ステップとを実行させ、
- 上記情報処理装置に、
- 上記記録再生装置との間の認証を行い、認証成立時にセッションキー
- 25 を生成する認証ステップと、
- コンテンツ情報を上記セッションキーでバス暗号化して上記記録再生



装置に送出するバス暗号化ステップとを実行させる記録方法のプログラム。

49. 記録媒体から情報を読み出し、記録媒体に情報を記録する記録再生装置と、上記記録再生装置が伝達ステップを介して接続される情報処理装置とを備え、管理機構が管理する第1の暗号化鍵と、記録媒体固有の第2の暗号化鍵と、記録の度に生成される第3の暗号化鍵とを使用したコンテンツ情報暗号化方法で暗号化されたコンテンツ情報を記録媒体に記録する記録方法のプログラムを格納した記録媒体であって、

上記記録再生装置に、

10 第1の暗号化鍵を保持する保持ステップと、

記録媒体に暗号化されて記録されている第2の暗号化鍵を再生し、上記第1の暗号化鍵で復号する第2の暗号化鍵復号ステップと、

第3の暗号化鍵を生成する第3の暗号化鍵生成ステップと、

上記第3の暗号化鍵を復号された第2の暗号化鍵で暗号化する暗号化  
15 ステップと、

情報処理装置との間の認証を行い、認証成立時にセッションキーを生成する認証ステップと、

上記暗号化されて記録されている第2の暗号化鍵を上記セッションキーによってバス暗号化して上記情報処理装置に伝送する第1のバス暗号  
20 化ステップと、

暗号化された上記第3の暗号化鍵を上記セッションキーによってバス暗号化して上記情報処理装置に伝送する第2のバス暗号化ステップと、

上記情報処理装置からの暗号化およびバス暗号化されたコンテンツ情報をバス復号するバス復号ステップと、

25 上記暗号化された上記第3の暗号化鍵と、上記暗号化されたコンテンツ情報を記録媒体に記録する記録ステップとを実行させ、

上記情報処理装置に、

第 1 の暗号化鍵を保持する保持ステップと、

上記記録再生装置との間の認証を行い、認証成立時にセッションキーを生成する認証ステップと、

- 5     上記バス暗号化された第 2 の暗号化鍵を上記セッションキーによってバス復号して暗号化された上記第 2 の暗号化鍵を復号する第 1 のバス復号ステップと、

      上記暗号化された第 2 の暗号化鍵を上記第 1 の暗号化鍵で復号する復号ステップと、

- 10    上記バス暗号化された第 3 の暗号化鍵を上記セッションキーによってバス復号して上記暗号化された第 3 の暗号化鍵を復号する第 2 のバス復号化ステップと、

      上記暗号化された第 3 の暗号化鍵を上記第 2 の暗号化鍵で復号する復号ステップと、

- 15    上記記録再生装置に対して伝送するコンテンツ情報を上記第 3 の暗号化で暗号化する暗号化ステップと、

      上記暗号化されたコンテンツ情報を上記セッションキーでバス暗号化して上記記録再生装置に送出するバス暗号化ステップとを実行させる記録方法のプログラムを格納した記録媒体。

- 20    50. 記録媒体から情報を読み出し、記録媒体に情報を記録する記録再生装置と、上記記録再生装置が伝達ステップを介して接続される情報処理装置とを備え、管理機構が管理する第 1 の暗号化鍵と、記録媒体固有の第 2 の暗号化鍵と、記録の度に生成される第 3 の暗号化鍵とを使用したコンテンツ情報暗号化方法で暗号化されたコンテンツ情報を記録媒体  
25    に記録する記録方法のプログラムを格納した記録媒体であって、

      上記記録再生装置に、

- 第 1 の暗号化鍵を保持する保持ステップと、  
第 2 の暗号化鍵を生成する第 2 の暗号化鍵生成ステップと、  
生成された第 2 の暗号化鍵を第 1 の暗号化鍵で暗号化する暗号化ステップと、
- 5 第 3 の暗号化鍵を生成する第 3 の暗号化鍵生成ステップと、  
生成された第 2 の暗号化鍵で上記第 3 の暗号化鍵を暗号化する暗号化ステップと、  
情報処理装置との間の認証を行い、認証成立時にセッションキーを生成する認証ステップと、
- 10 上記暗号化された第 2 の暗号化鍵を上記セッションキーによってバス暗号化して上記情報処理装置に伝送する第 1 のバス暗号化ステップと、  
暗号化された上記第 3 の暗号化鍵を上記セッションキーによってバス暗号化して上記情報処理装置に伝送する第 2 のバス暗号化ステップと、  
上記情報処理装置からの暗号化およびバス暗号化されたコンテンツ情報
- 15 報をバス復号するバス復号ステップと、  
上記暗号化された上記第 2 の暗号化鍵と、上記暗号化された上記第 3 の暗号化鍵と、上記暗号化されたコンテンツ情報を記録媒体に記録する記録ステップとを実行させ、  
上記情報処理装置に、
- 20 第 1 の暗号化鍵を保持する保持ステップと、  
上記記録再生装置との間の認証を行い、認証成立時にセッションキーを生成する認証ステップと、  
上記バス暗号化された第 2 の暗号化鍵を上記セッションキーによってバス復号して暗号化された上記第 2 の暗号化鍵を復号する第 1 のバス復
- 25 号ステップと、  
上記暗号化された第 2 の暗号化鍵を上記第 1 の暗号化鍵で復号する復

号ステップと、

上記バス暗号化された第 3 の暗号化鍵を上記セッションキーによってバス復号して上記暗号化された第 3 の暗号化鍵を復号する第 2 のバス復号化ステップと、

- 5     上記暗号化された第 3 の暗号化鍵を上記第 2 の暗号化鍵で復号する復号ステップと、

上記記録再生装置に対して伝送するコンテンツ情報を上記第 3 の暗号化で暗号化する暗号化ステップと、

- 10    上記暗号化されたコンテンツ情報を上記セッションキーでバス暗号化して上記記録再生装置に送出するバス暗号化ステップとを実行させる記録方法のプログラムを格納した記録媒体。

- 5 1. 記録媒体から情報を読み出し、記録媒体に情報を記録する記録再生装置と、上記記録再生装置が伝達ステップを介して接続される情報処理装置とを備え、管理機構が管理する第 1 の暗号化鍵と、記録媒体固有の第 2 の暗号化鍵と、記録の度に生成される第 3 の暗号化鍵とを使用したコンテンツ情報暗号化方法で暗号化されたコンテンツ情報を記録媒体に記録する記録方法のプログラムを格納した記録媒体であって、

上記記録再生装置に、

第 1 の暗号化鍵を保持する保持ステップと、

- 20    記録媒体に暗号化されて記録されている第 2 の暗号化鍵を再生し、上記第 1 の暗号化鍵で復号する第 2 の暗号化鍵復号ステップと、

第 3 の暗号化鍵を生成する第 3 の暗号化鍵生成ステップと、

第 3 の暗号化鍵を復号された第 2 の暗号化鍵で暗号化する暗号化ステップと、

- 25    情報処理装置との間の認証を行い、認証成立時にセッションキーを生成する認証ステップと、

上記情報処理装置からのバス暗号化されたコンテンツ情報をバス復号するバス復号ステップと、

上記コンテンツ情報を上記第 3 の暗号化鍵によって暗号化する暗号化ステップと、

- 5     上記暗号化された上記第 3 の暗号化鍵と、上記暗号化されたコンテンツ情報を記録媒体に記録する記録ステップとを実行させ、

上記情報処理装置に、

上記記録再生装置との間の認証を行い、認証成立時にセッションキーを生成する認証ステップと、

- 10    上記記録再生装置に対して伝送するコンテンツ情報を上記セッションキーでバス暗号化して上記記録再生装置に送出するバス暗号化ステップとを実行させる記録方法のプログラムを格納した記録媒体。

52. 記録媒体から情報を読み出し、記録媒体に情報を記録する記録再生装置と、上記記録再生装置が伝達ステップを介して接続される情報処

- 15    理装置とを備え、管理機構が管理する第 1 の暗号化鍵と、記録媒体固有の第 2 の暗号化鍵と、記録の度に生成される第 3 の暗号化鍵とを使用したコンテンツ情報暗号化方法で暗号化されたコンテンツ情報を記録媒体に記録する記録方法のプログラムを格納した記録媒体であって、

上記記録再生装置に、

- 20    第 1 の暗号化鍵を保持する保持ステップと、

第 2 の暗号化鍵を生成する第 2 の暗号化鍵生成ステップと、

生成された第 2 の暗号化鍵を上記第 1 の暗号化鍵で暗号化する暗号化ステップと、

第 3 の暗号化鍵を生成する第 3 の暗号化鍵生成ステップと、

- 25    上記第 3 の暗号化鍵を生成された第 2 の暗号化鍵で暗号化する暗号化ステップと、

情報処理装置との間の認証を行い、認証成立時にセッションキーを生成する認証ステップと、

上記情報処理装置からのバス暗号化されたコンテンツ情報をバス復号するバス復号ステップと、

- 5     上記コンテンツ情報を上記第 3 の暗号化鍵によって暗号化する暗号化ステップと、

上記暗号化された上記第 2 の暗号化鍵と、上記暗号化された上記第 3 の暗号化鍵と、上記暗号化されたコンテンツ情報を記録媒体に記録する記録ステップとを実行させ、

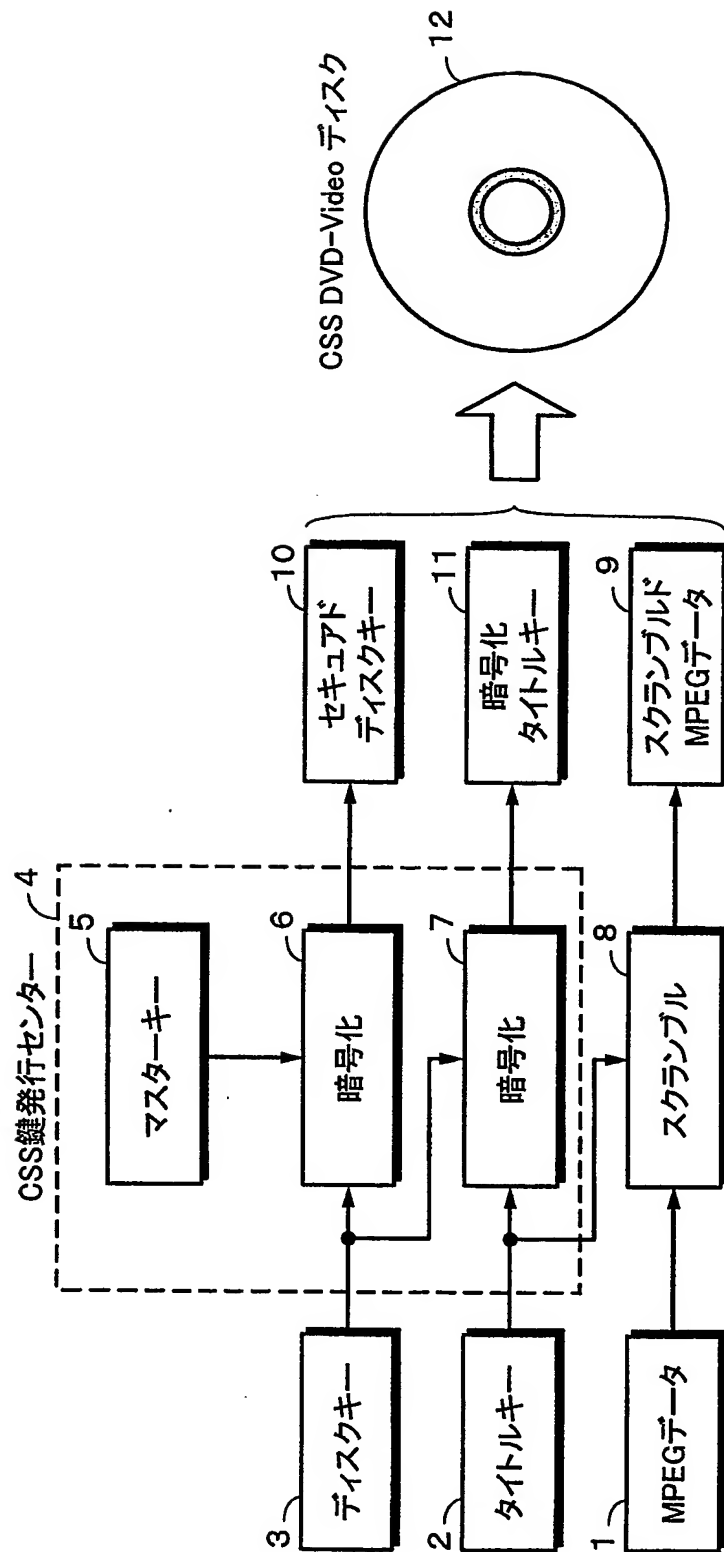
- 10    上記情報処理装置に、

上記記録再生装置との間の認証を行い、認証成立時にセッションキーを生成する認証ステップと、

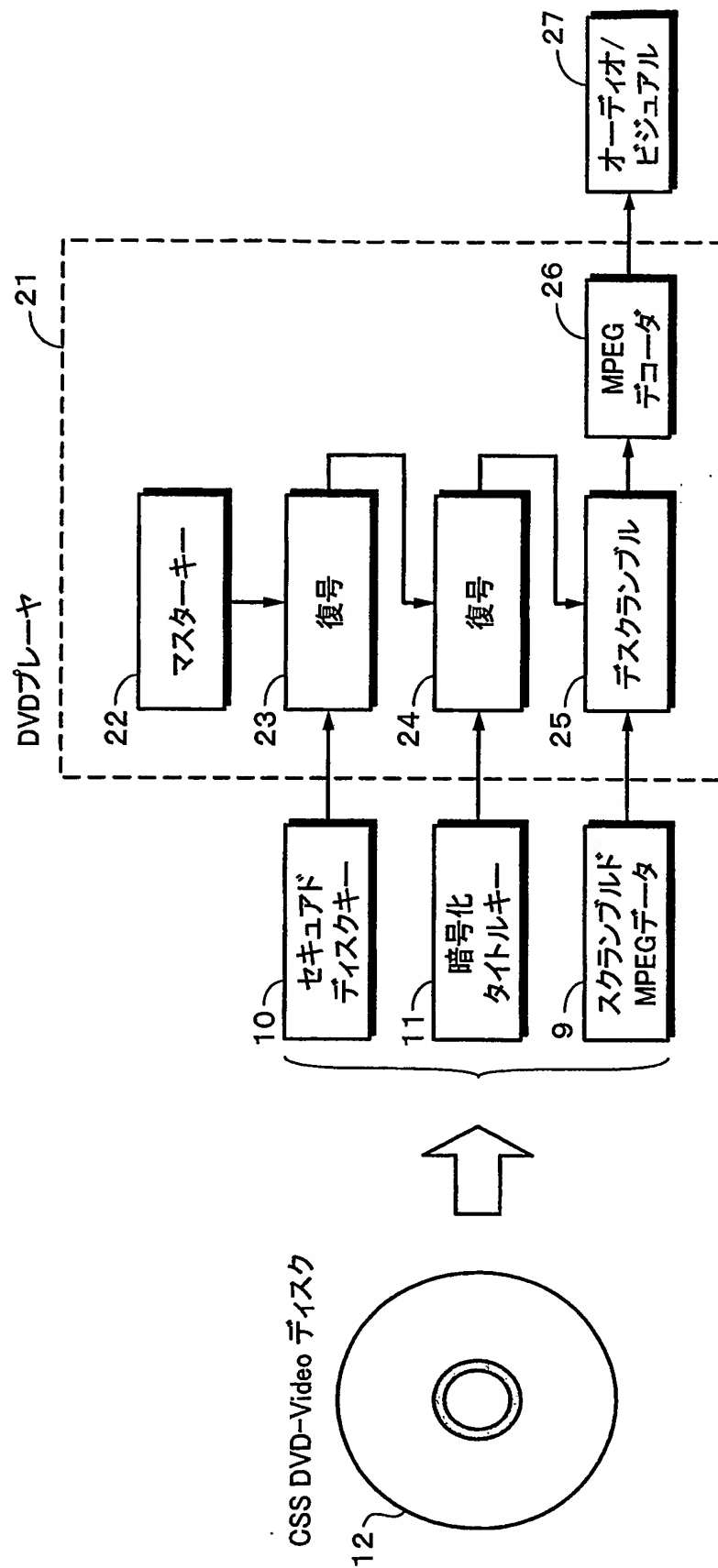
コンテンツ情報を上記セッションキーでバス暗号化して上記記録再生装置に送出するバス暗号化ステップとを実行させる記録方法のプログラ

- 15    ムを格納した記録媒体。

第1図

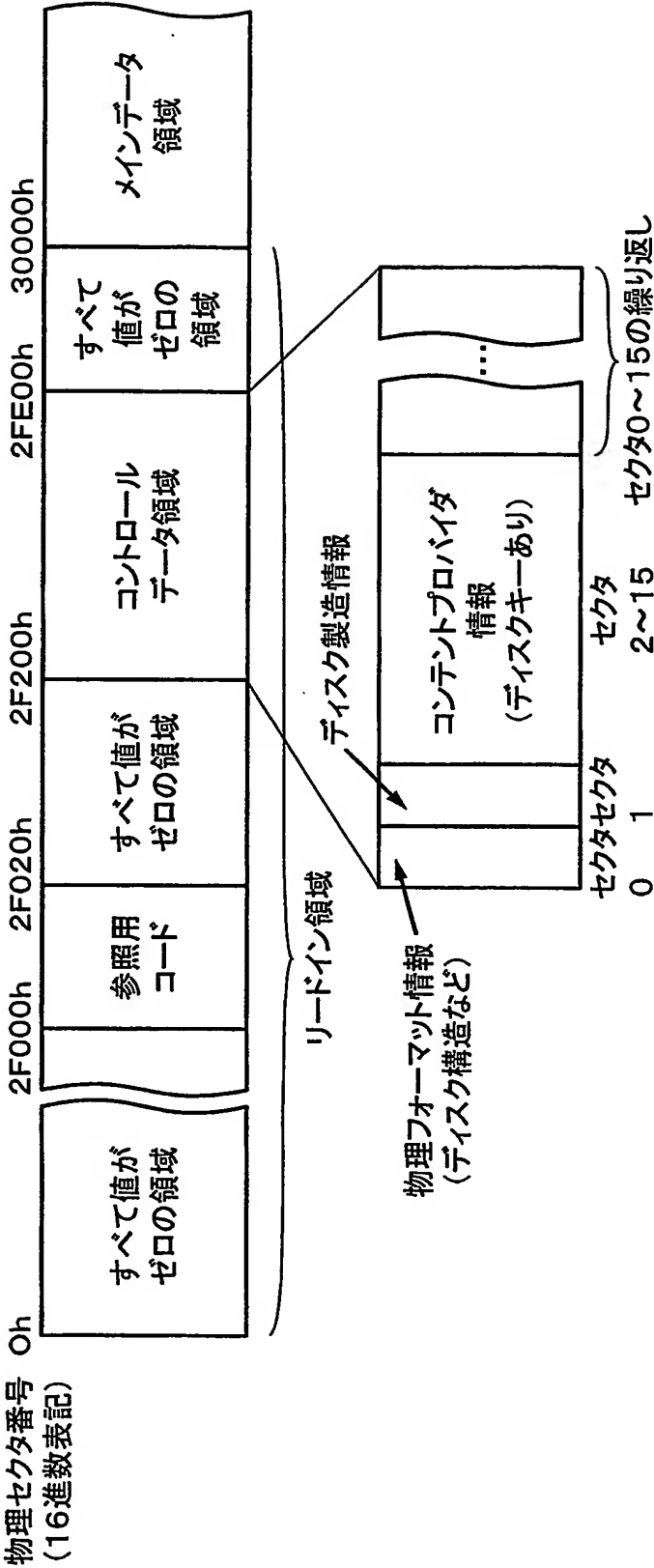


第2図

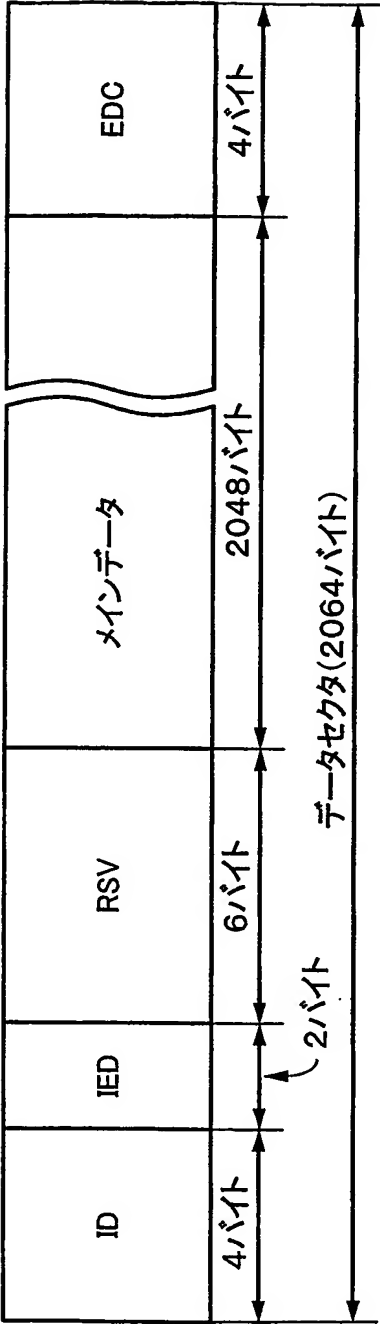




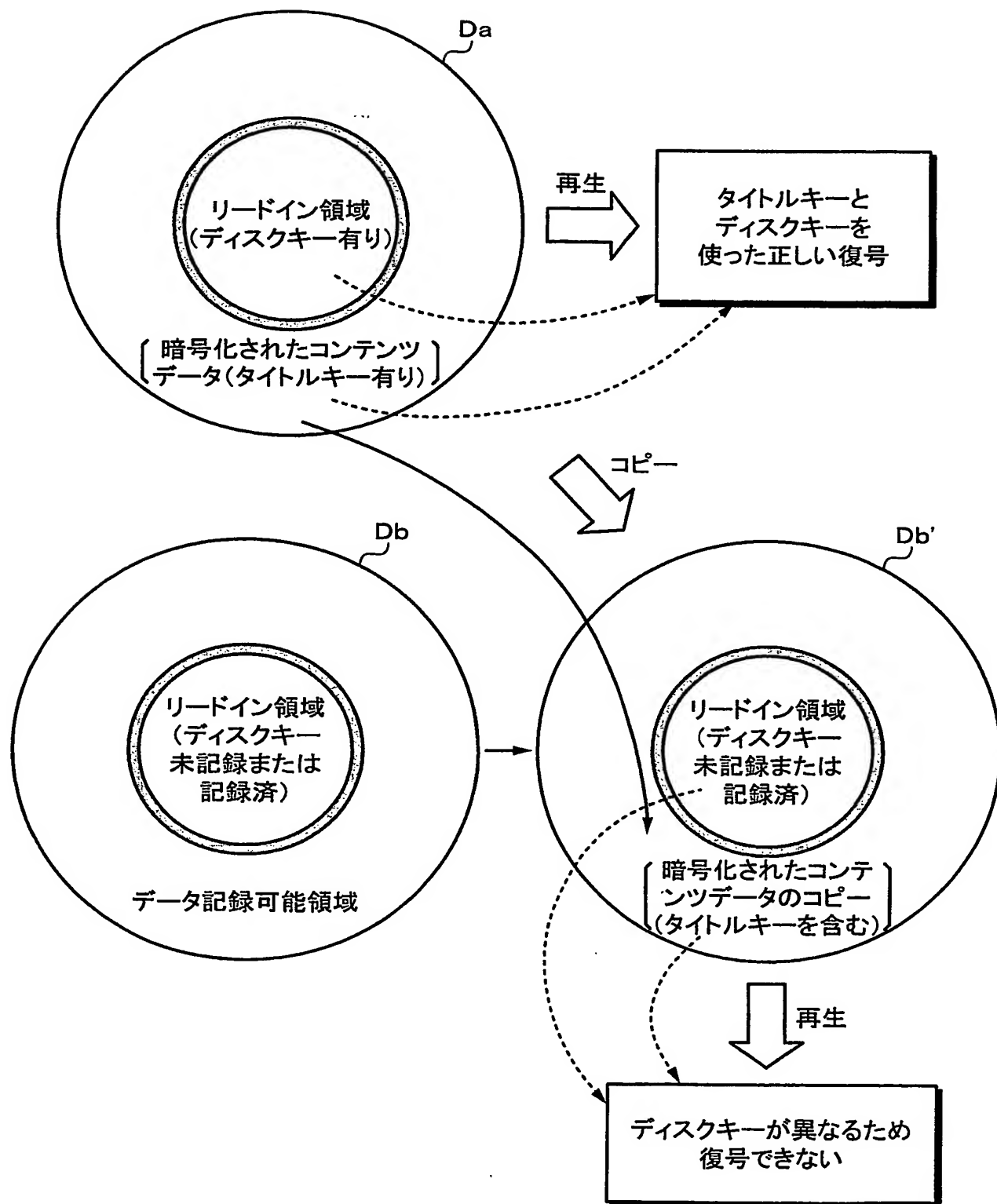
第3図



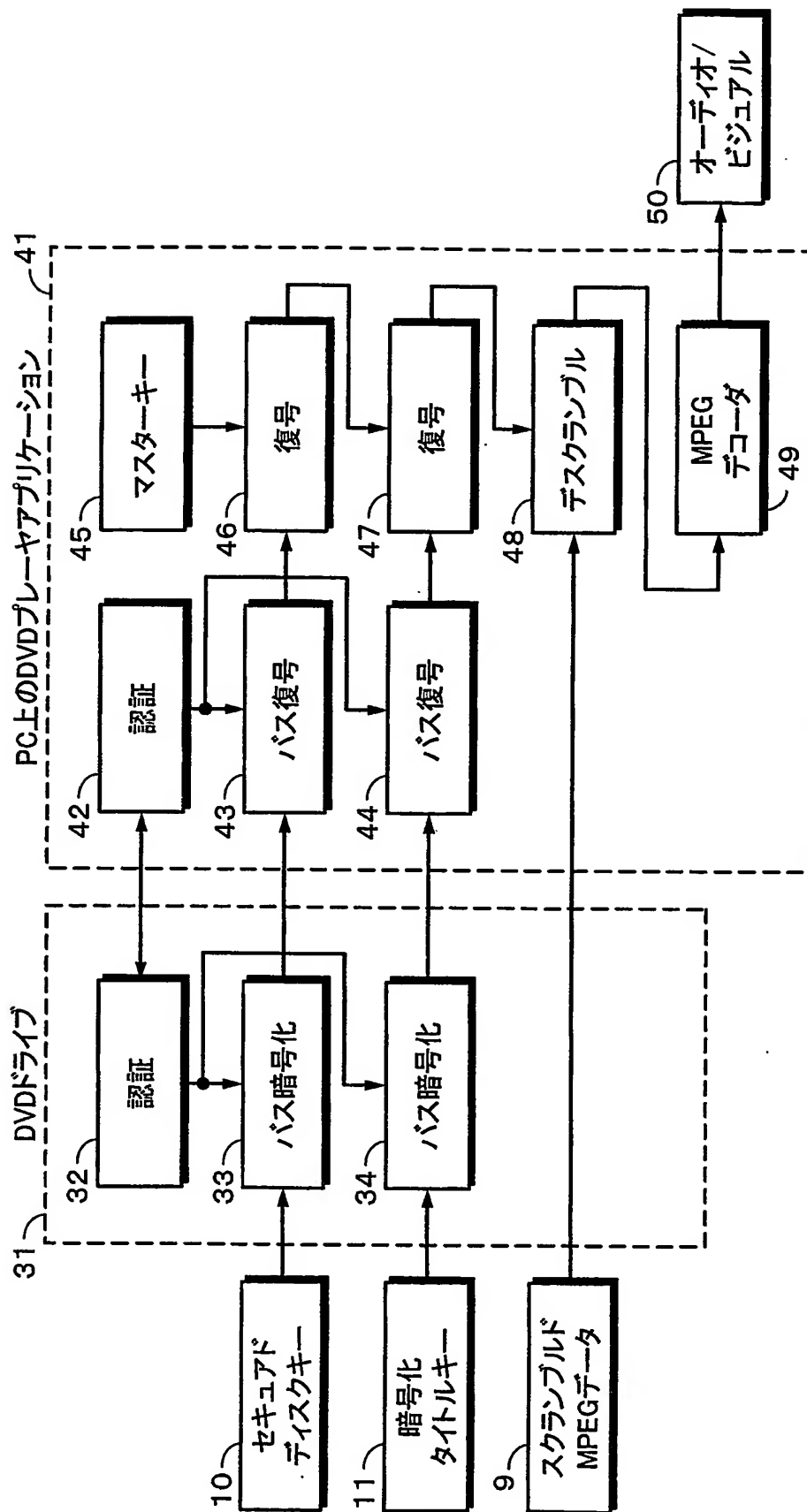
第4図



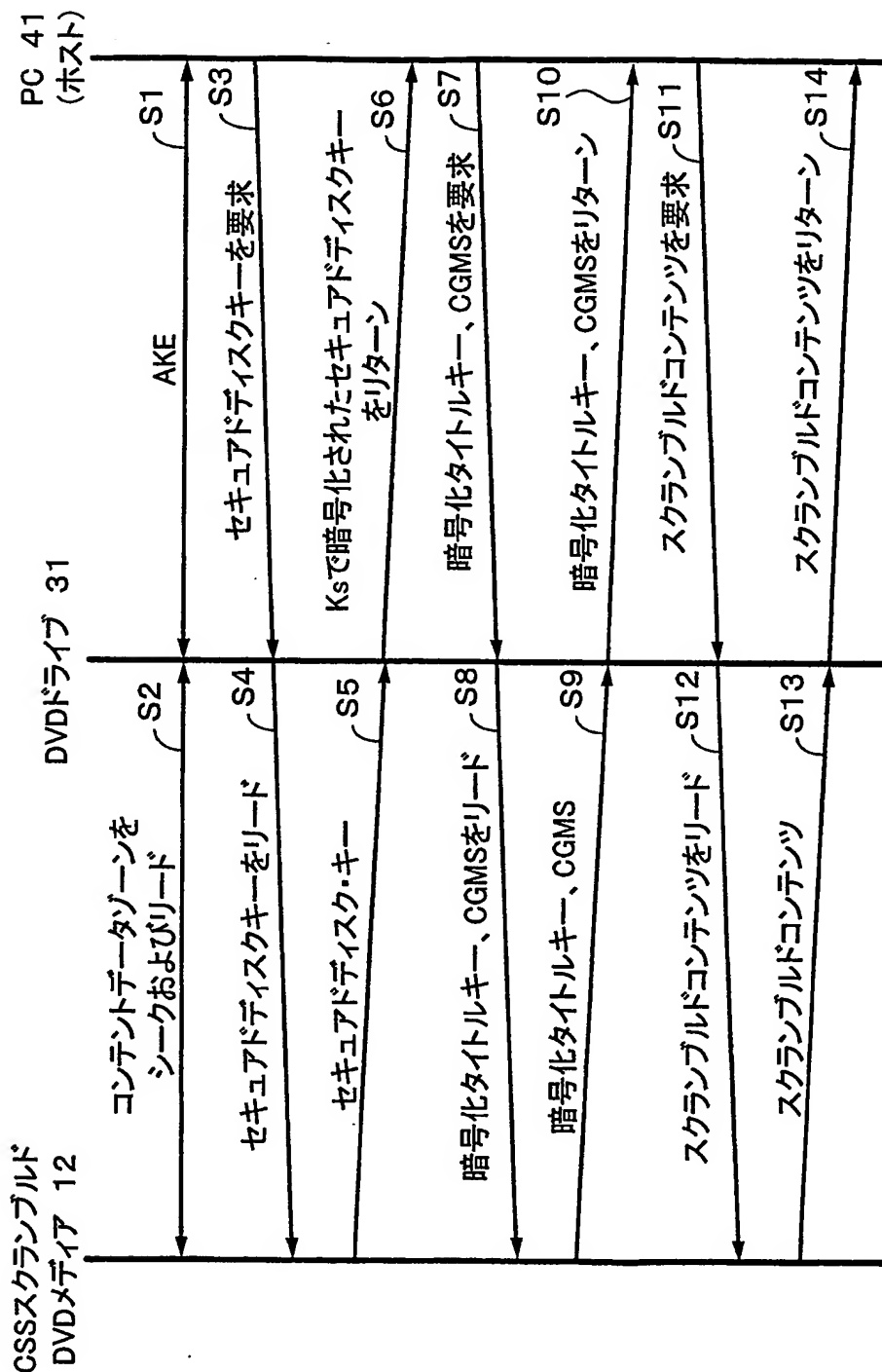
## 第5図



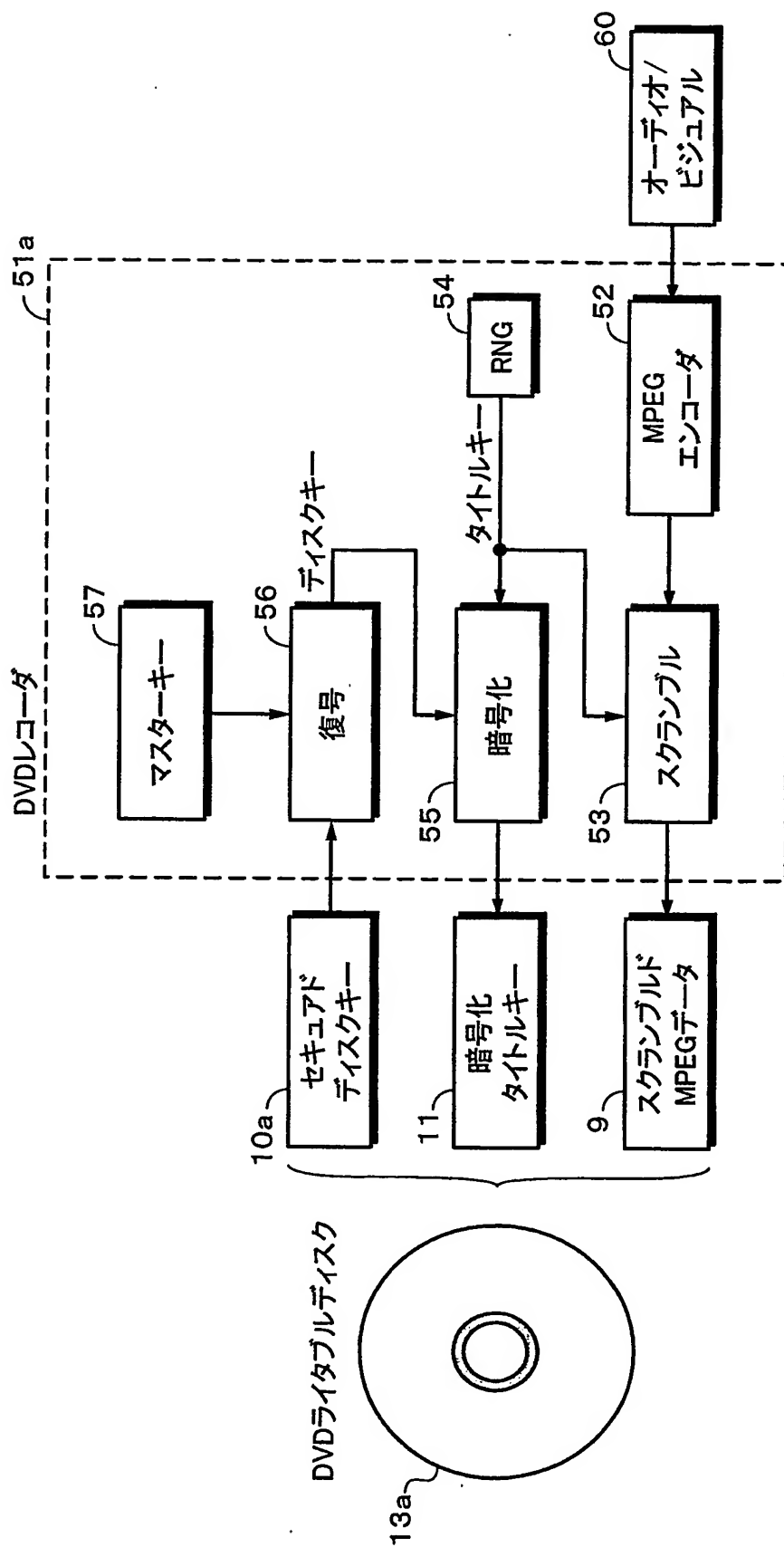
第6図



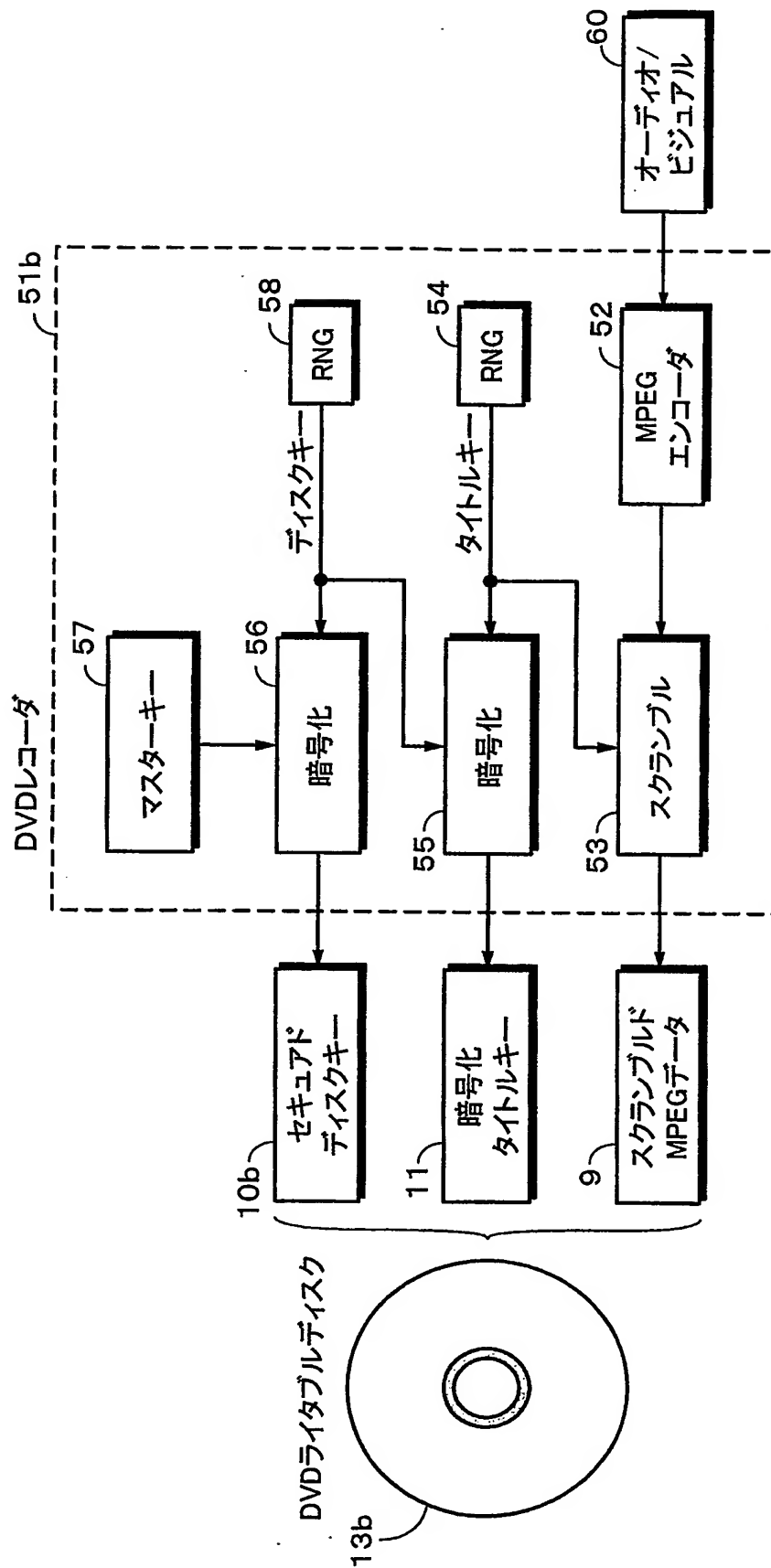
# 第7図



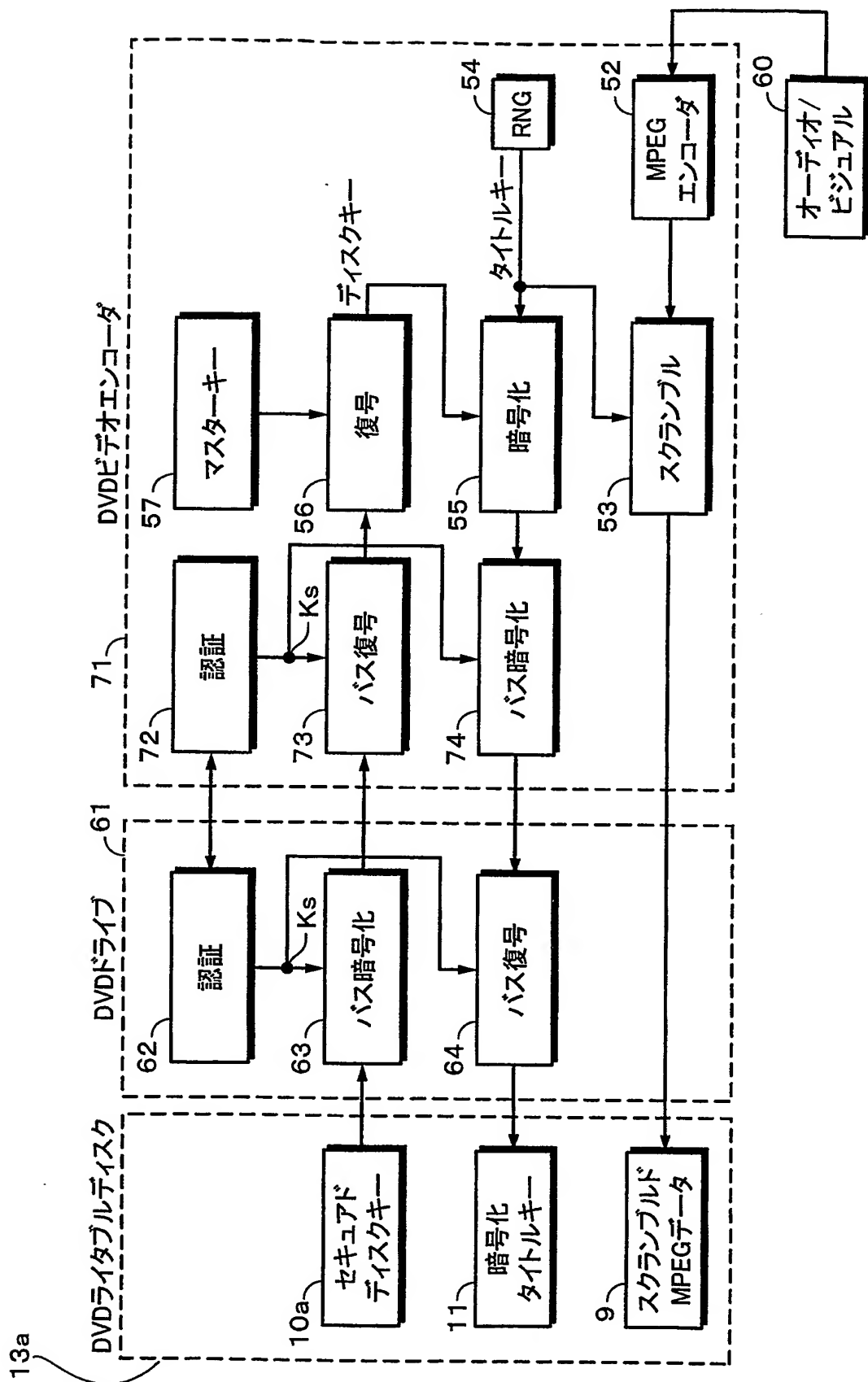
第8図



第9図

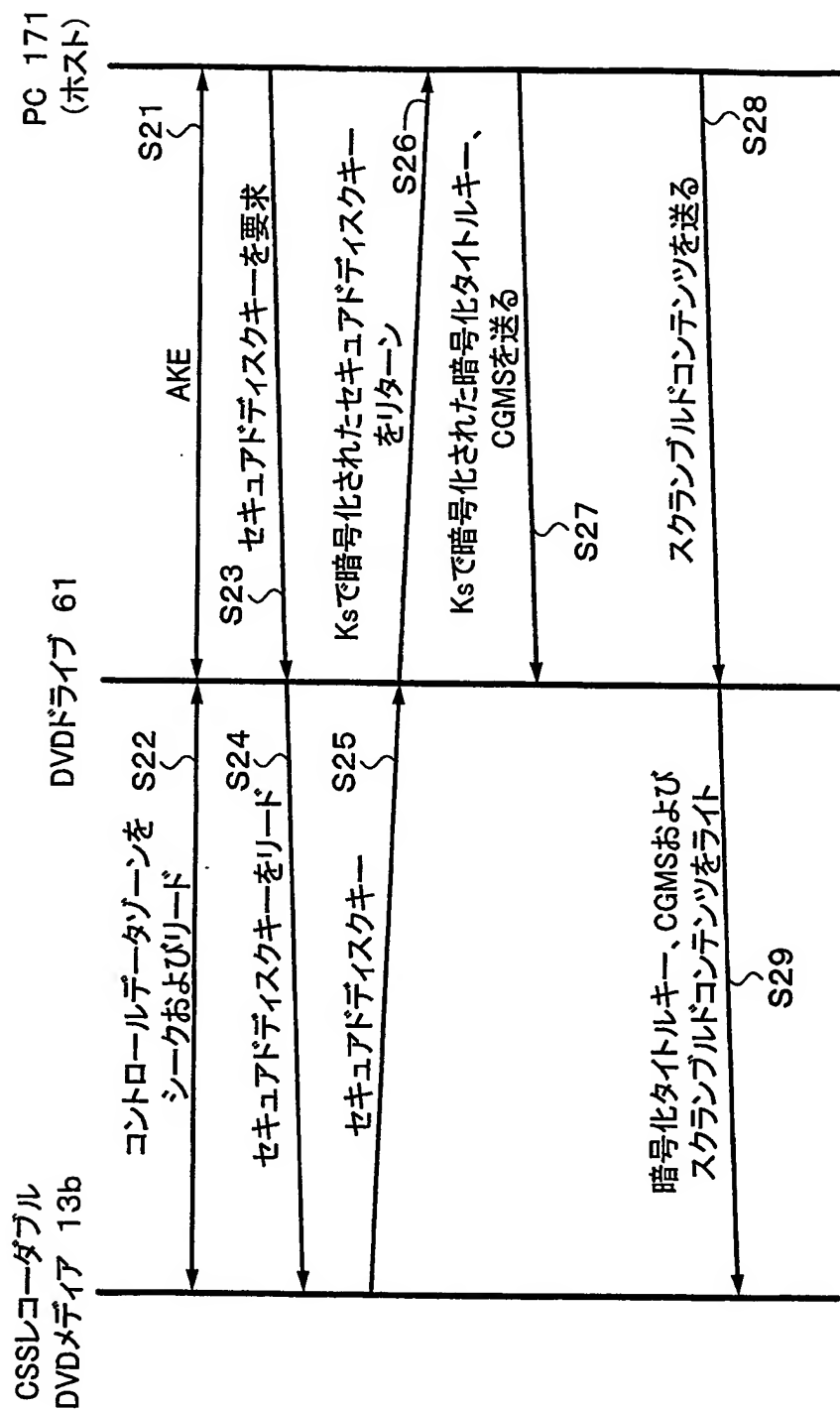


第10図

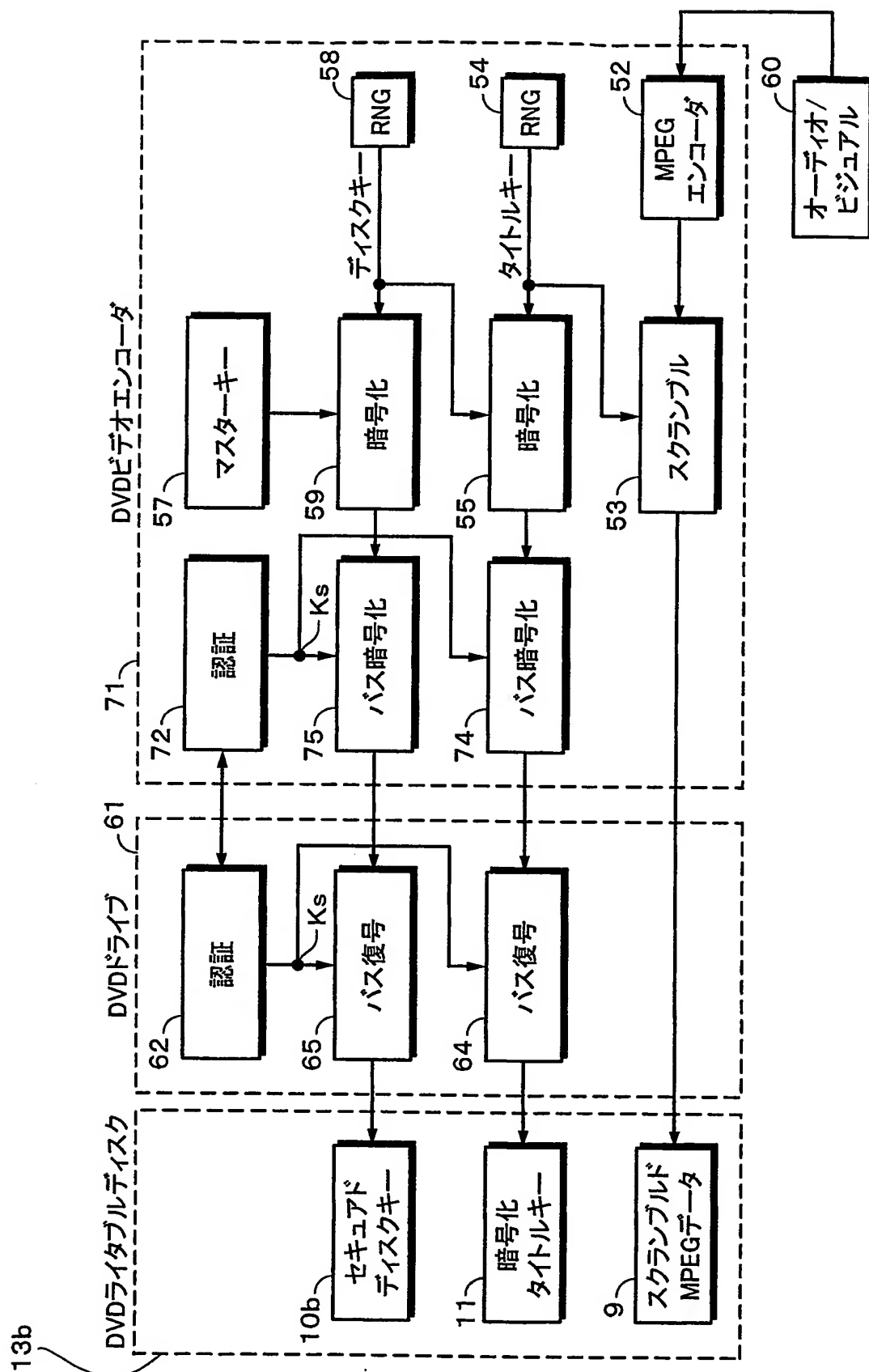




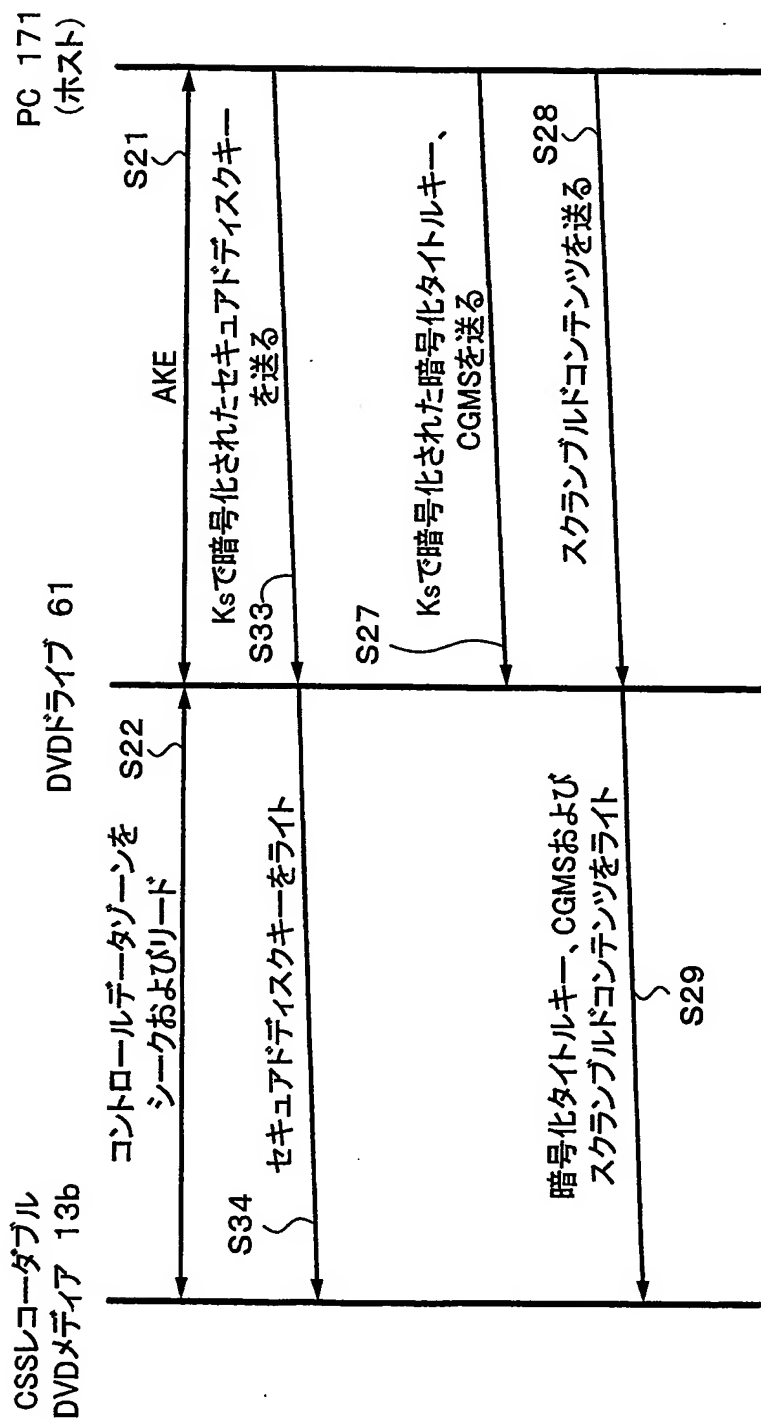
# 第11図



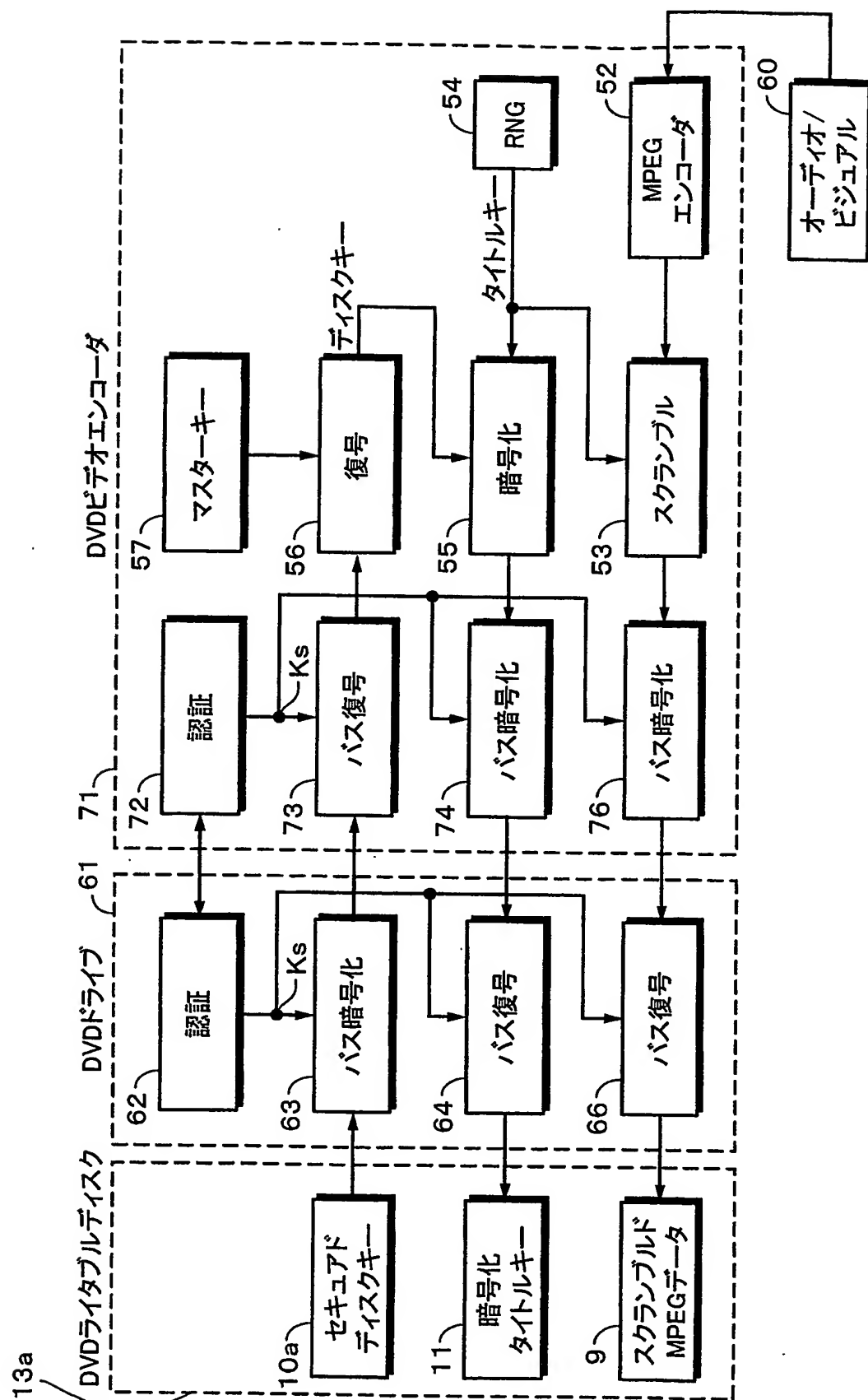
## 第12図



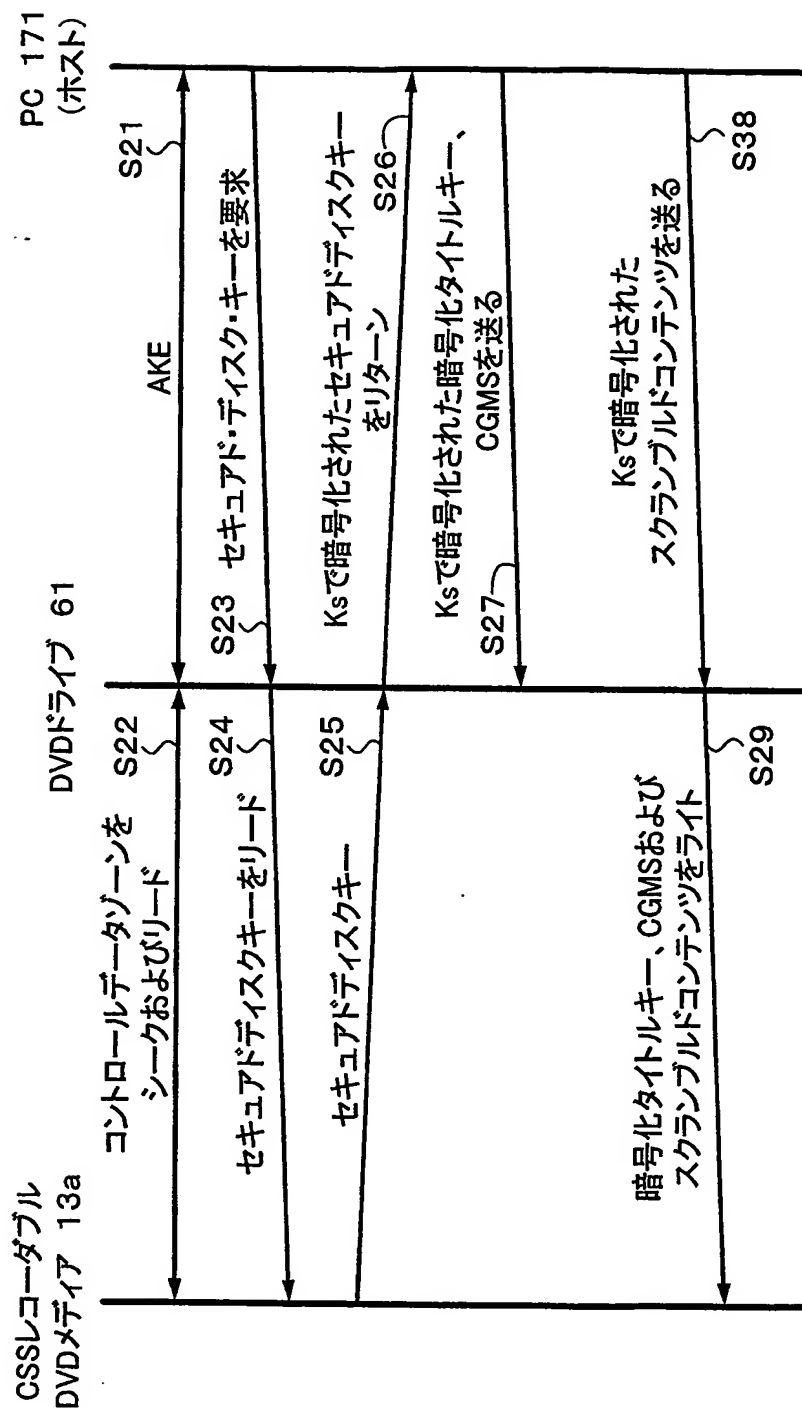
## 第13図



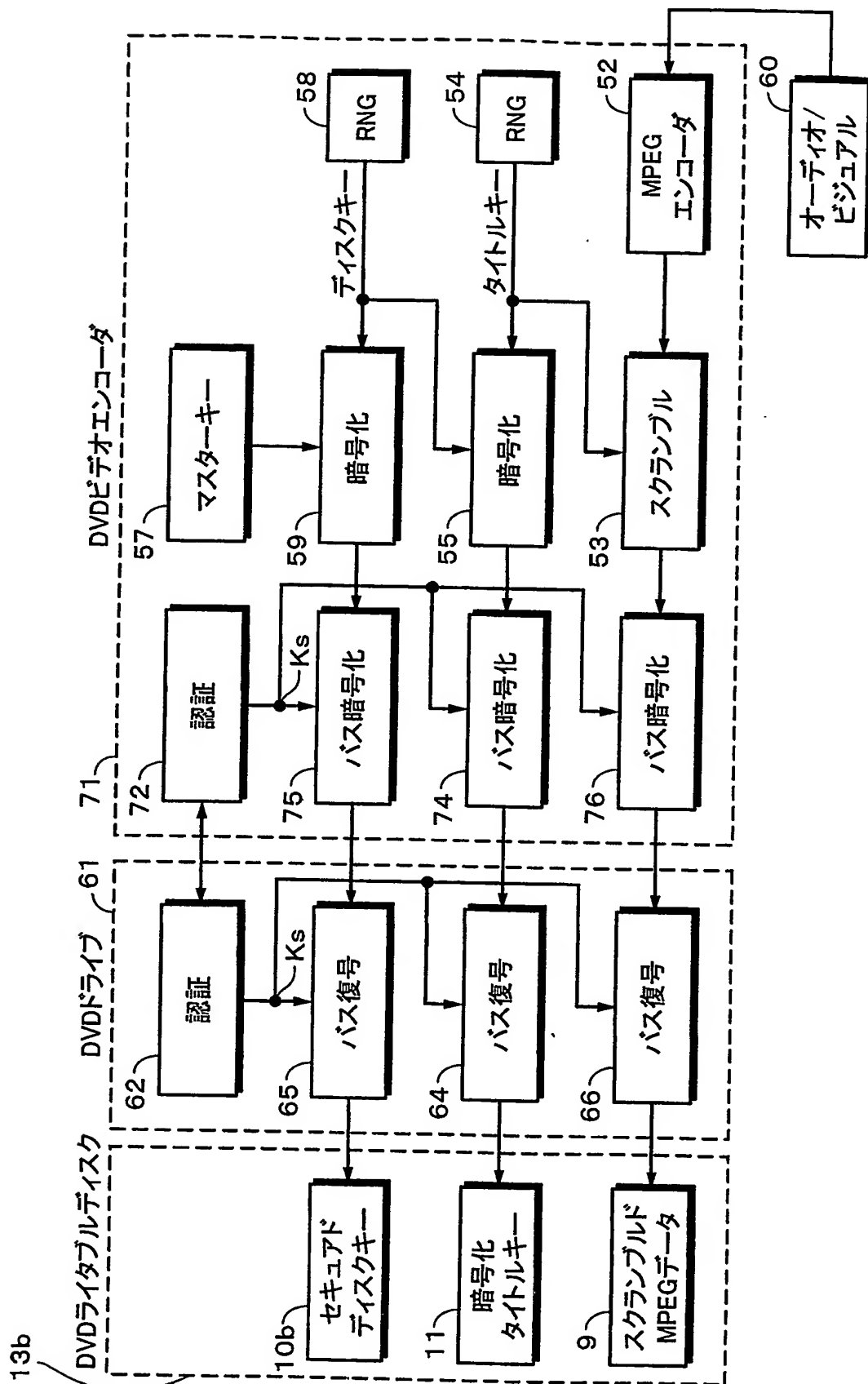
## 第14図



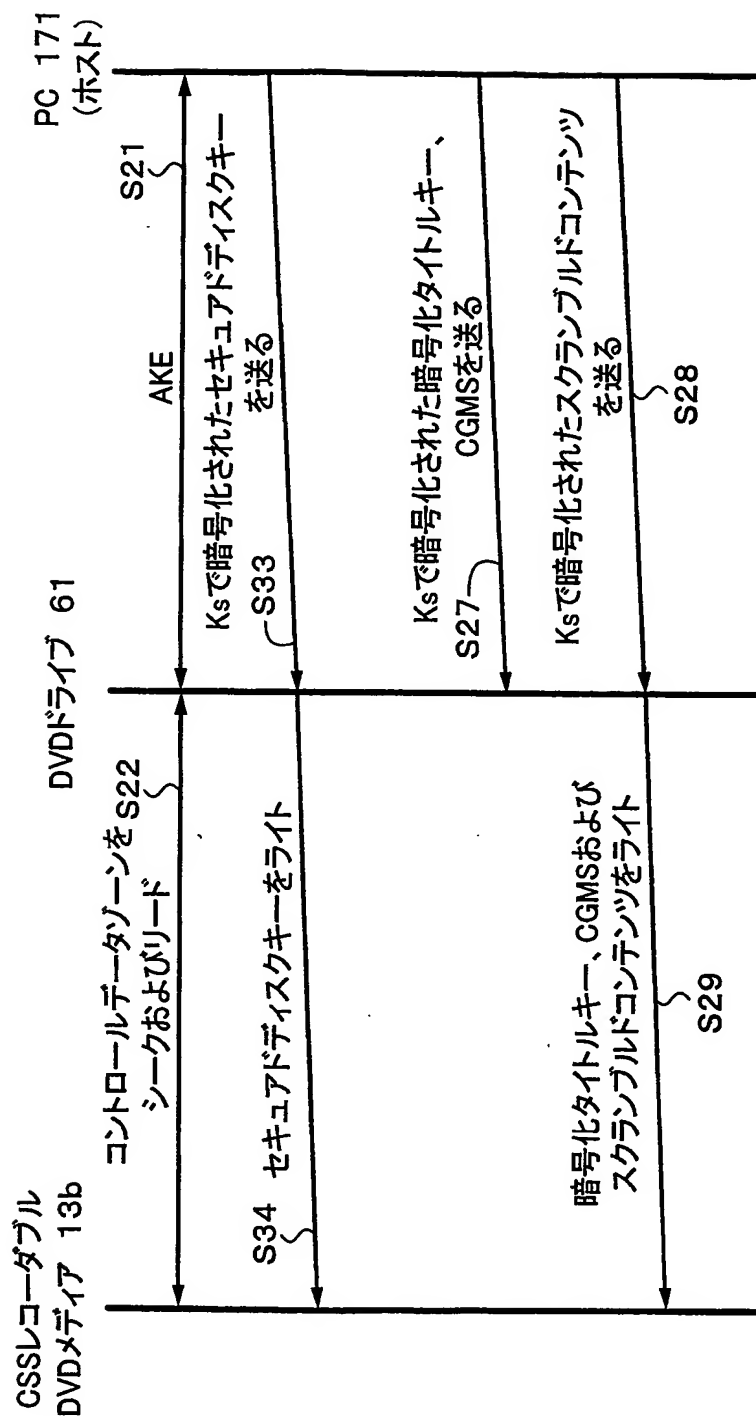
## 第15図



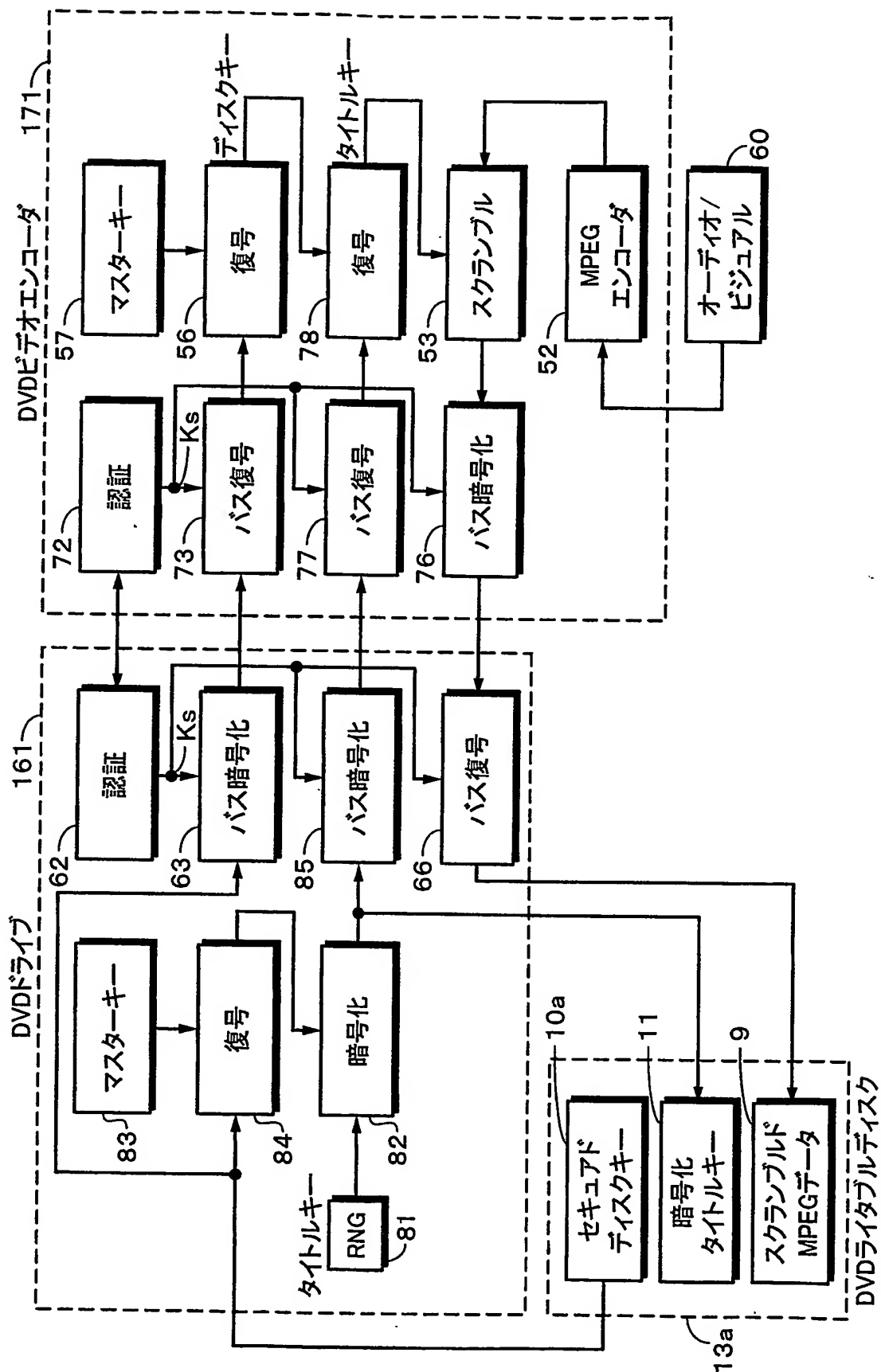
第16図



## 第17図

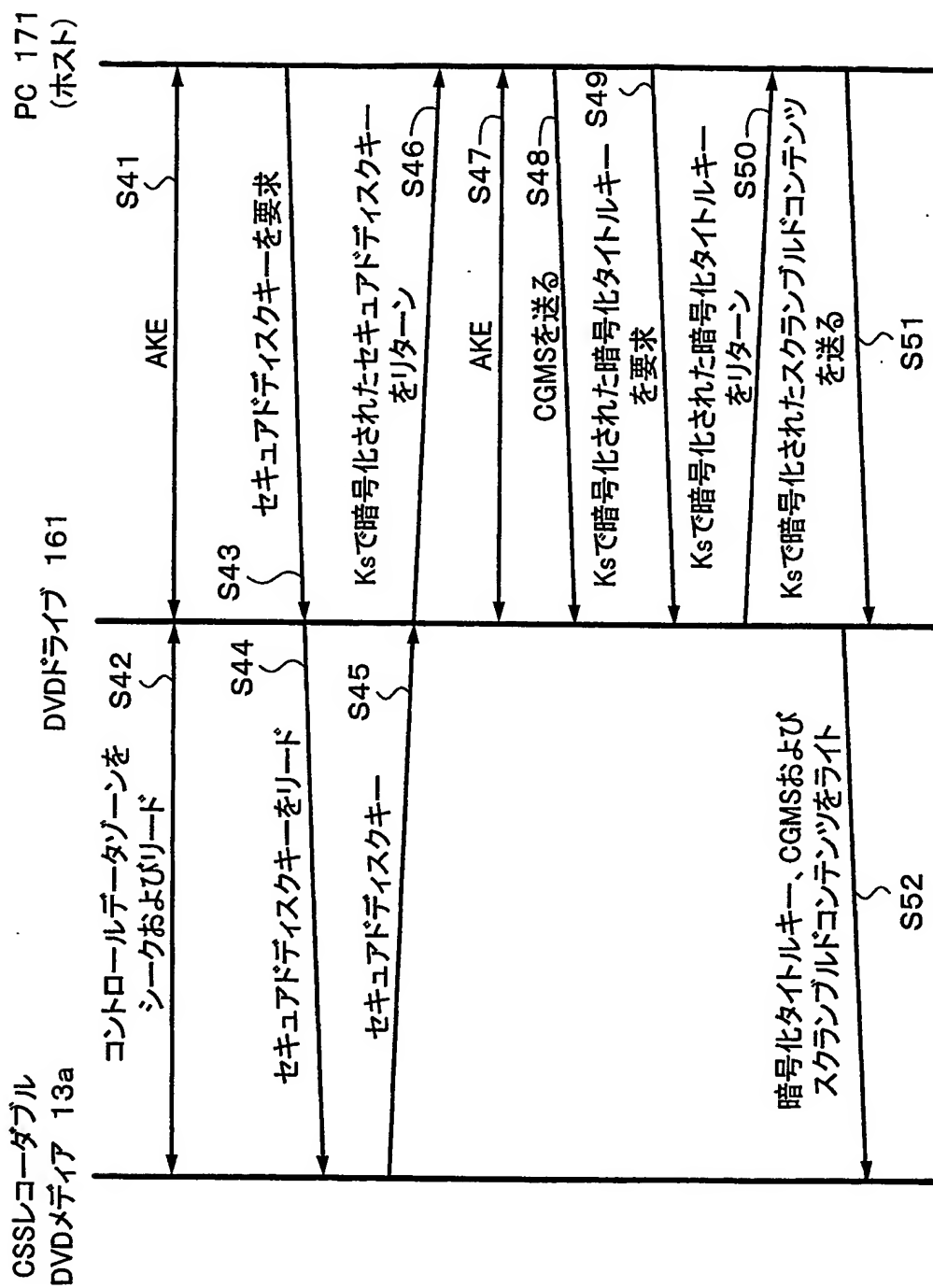


## 第18図

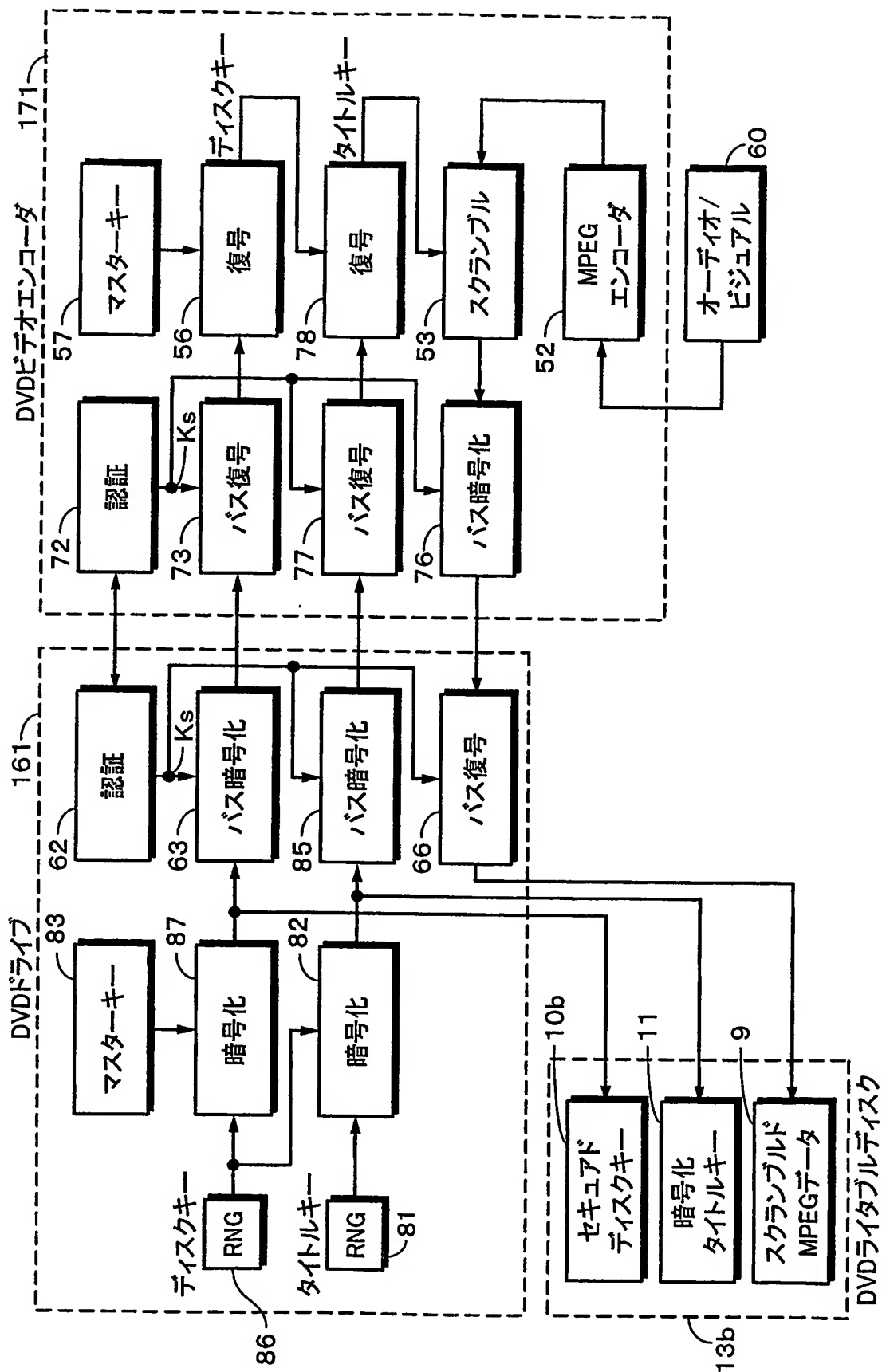




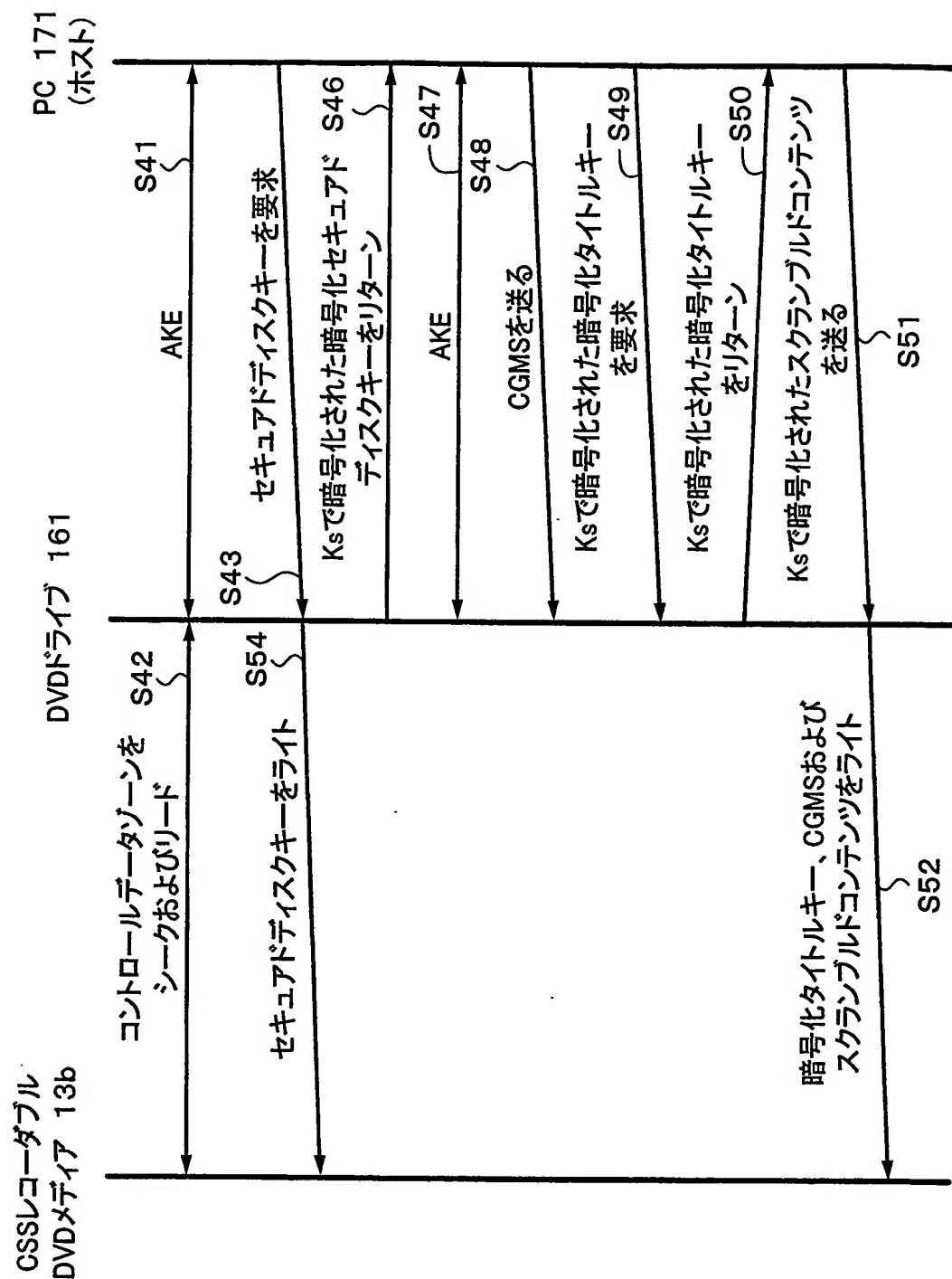
## 第19図



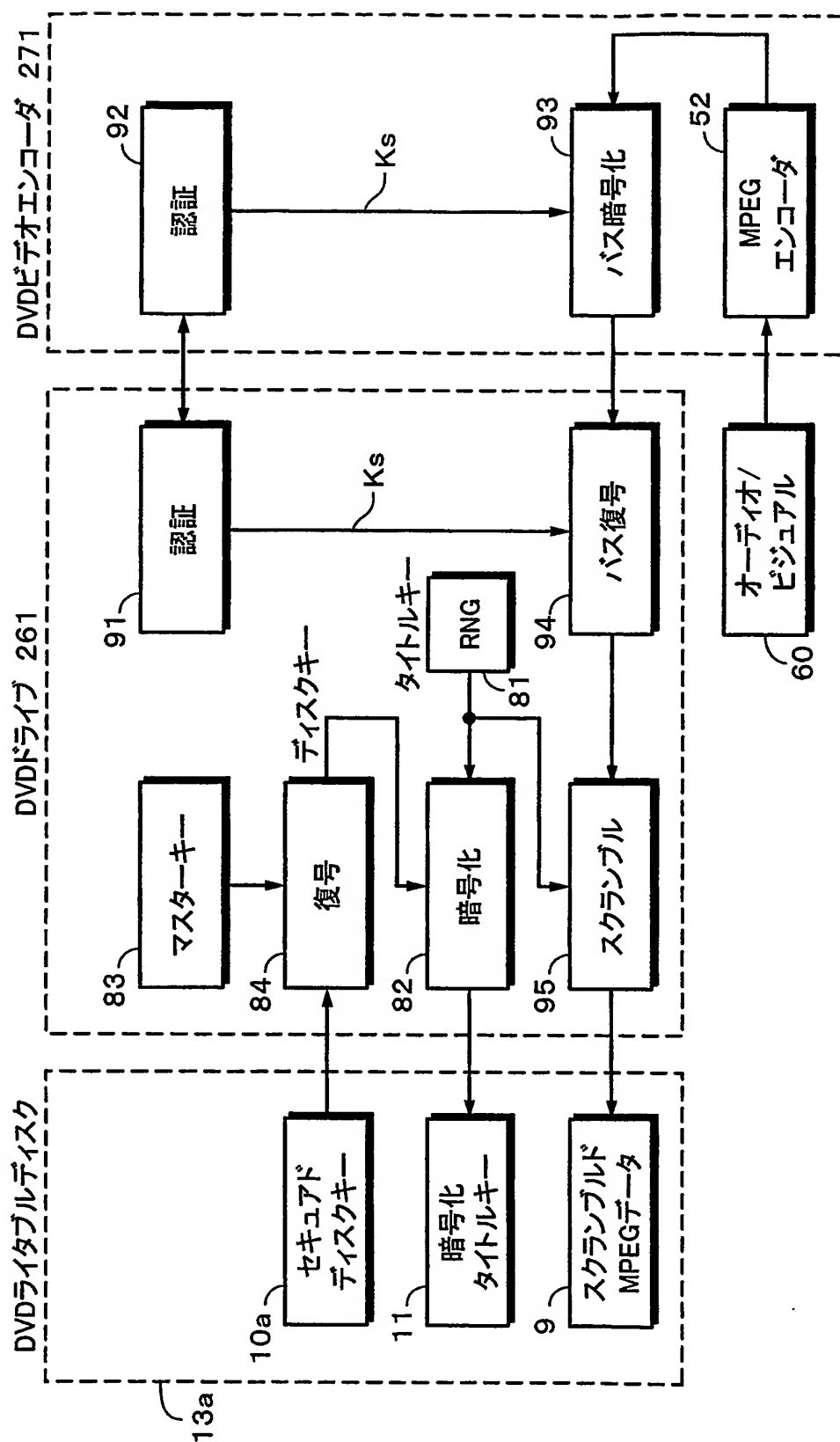
第20圖



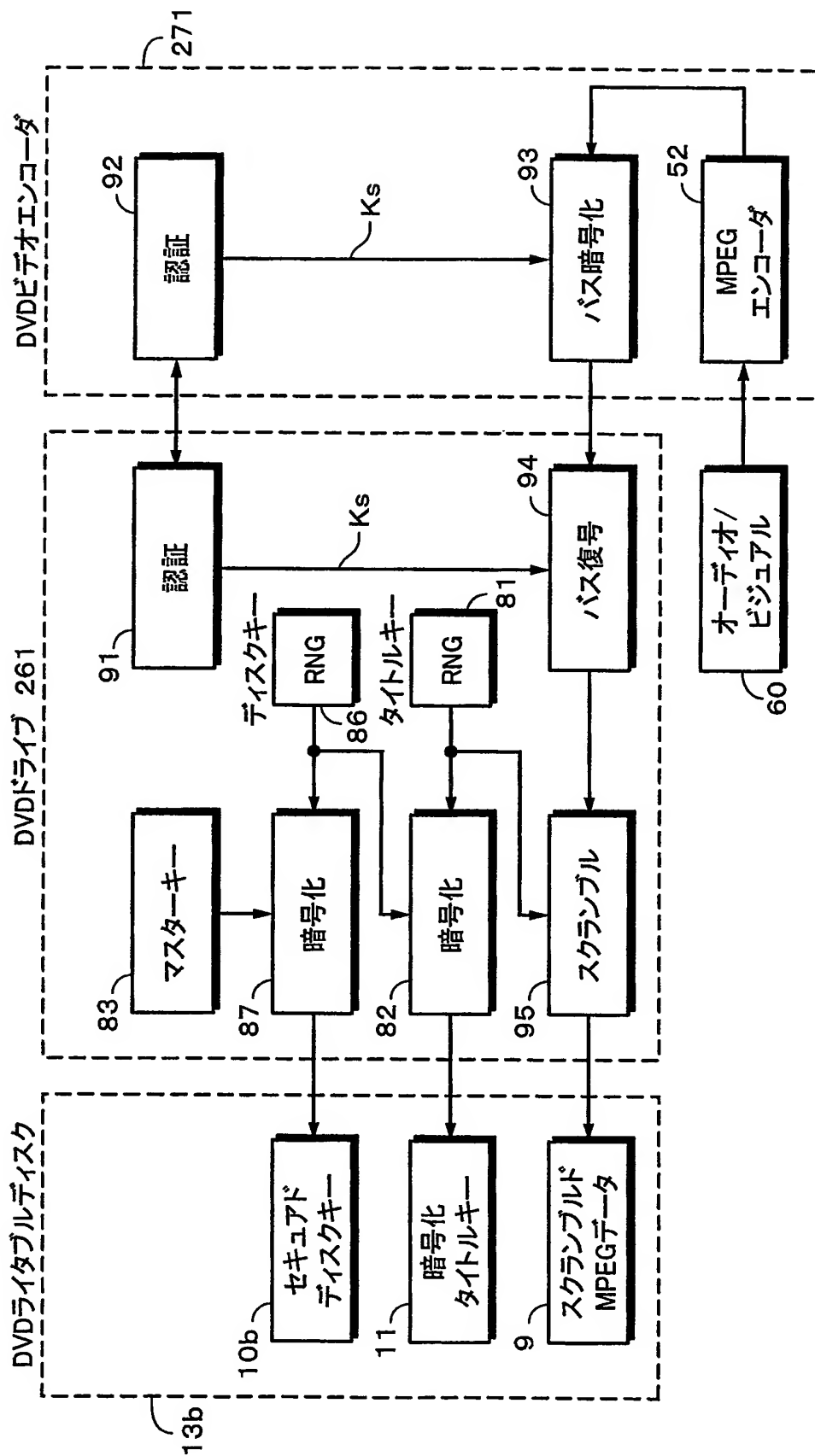
## 第21図



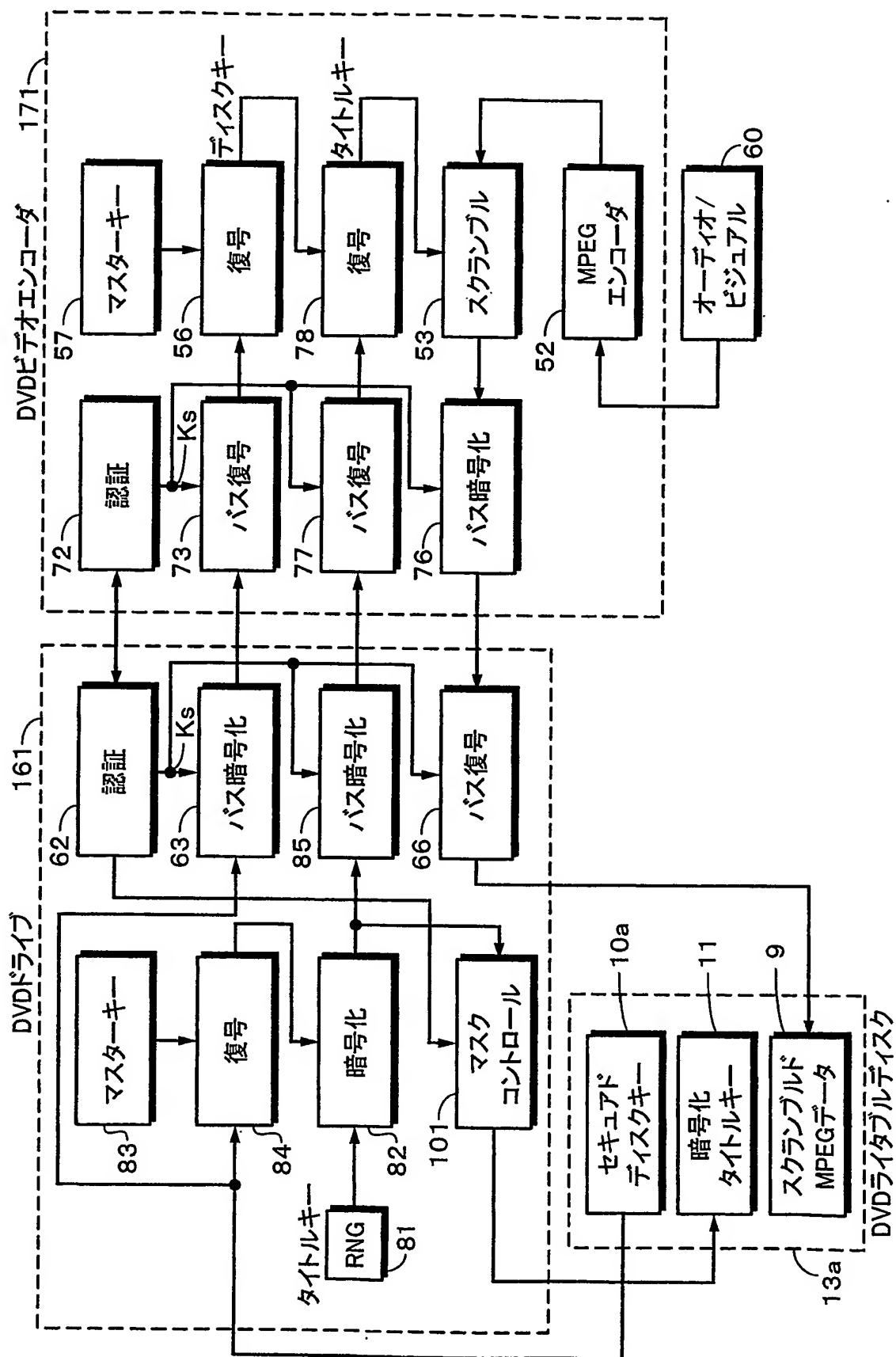
# 第22図



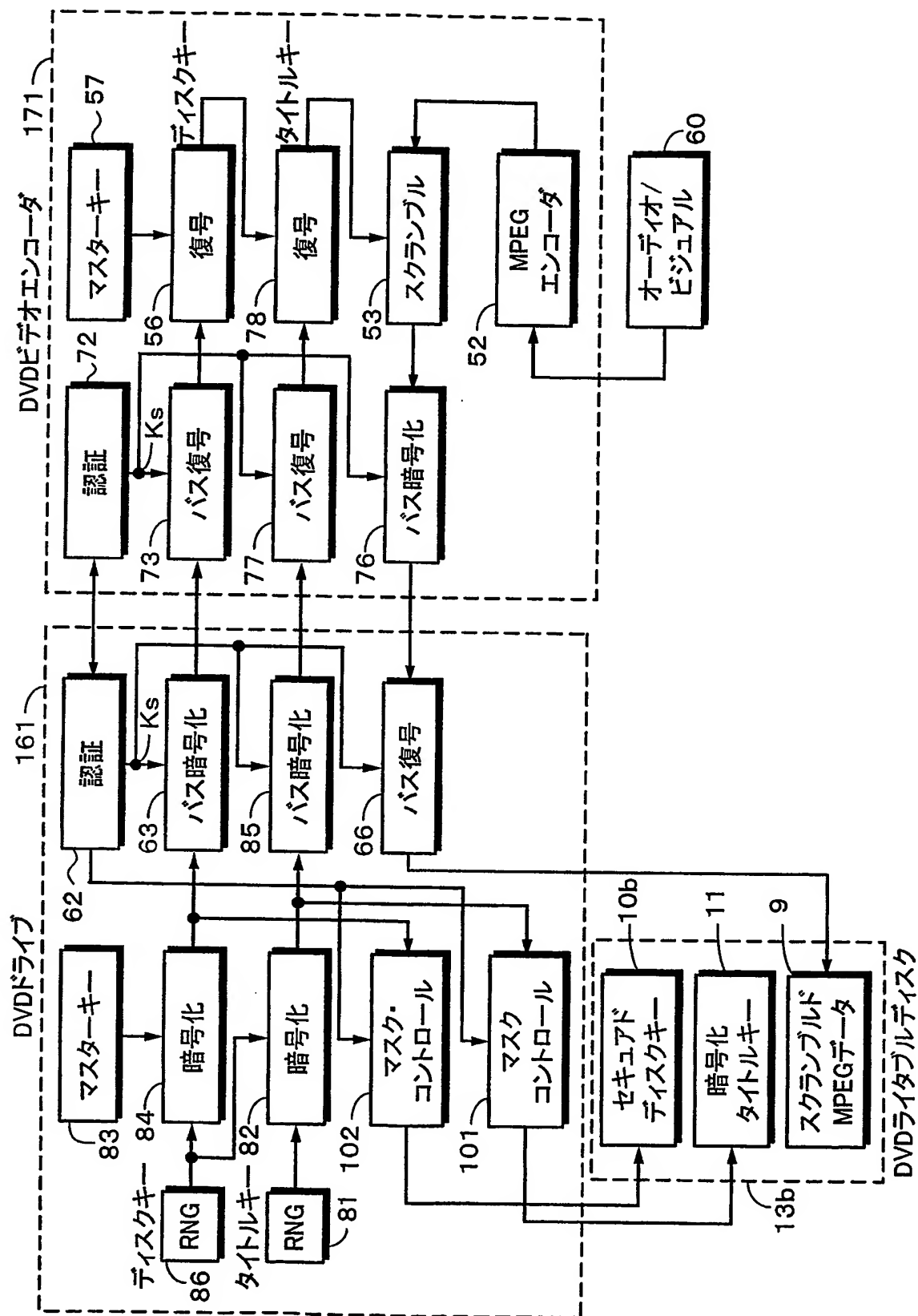
第23図



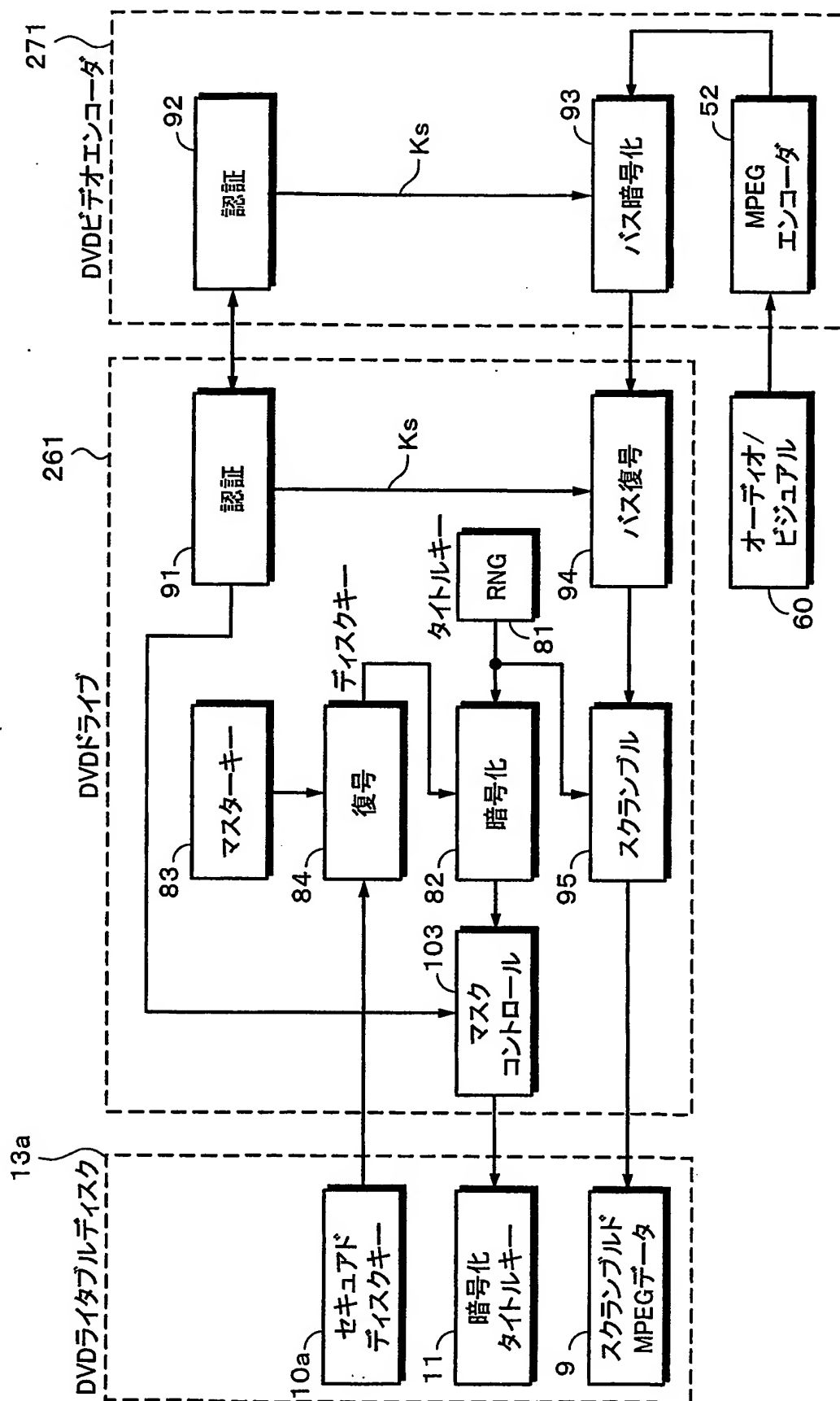
## 第24図



## 第25図

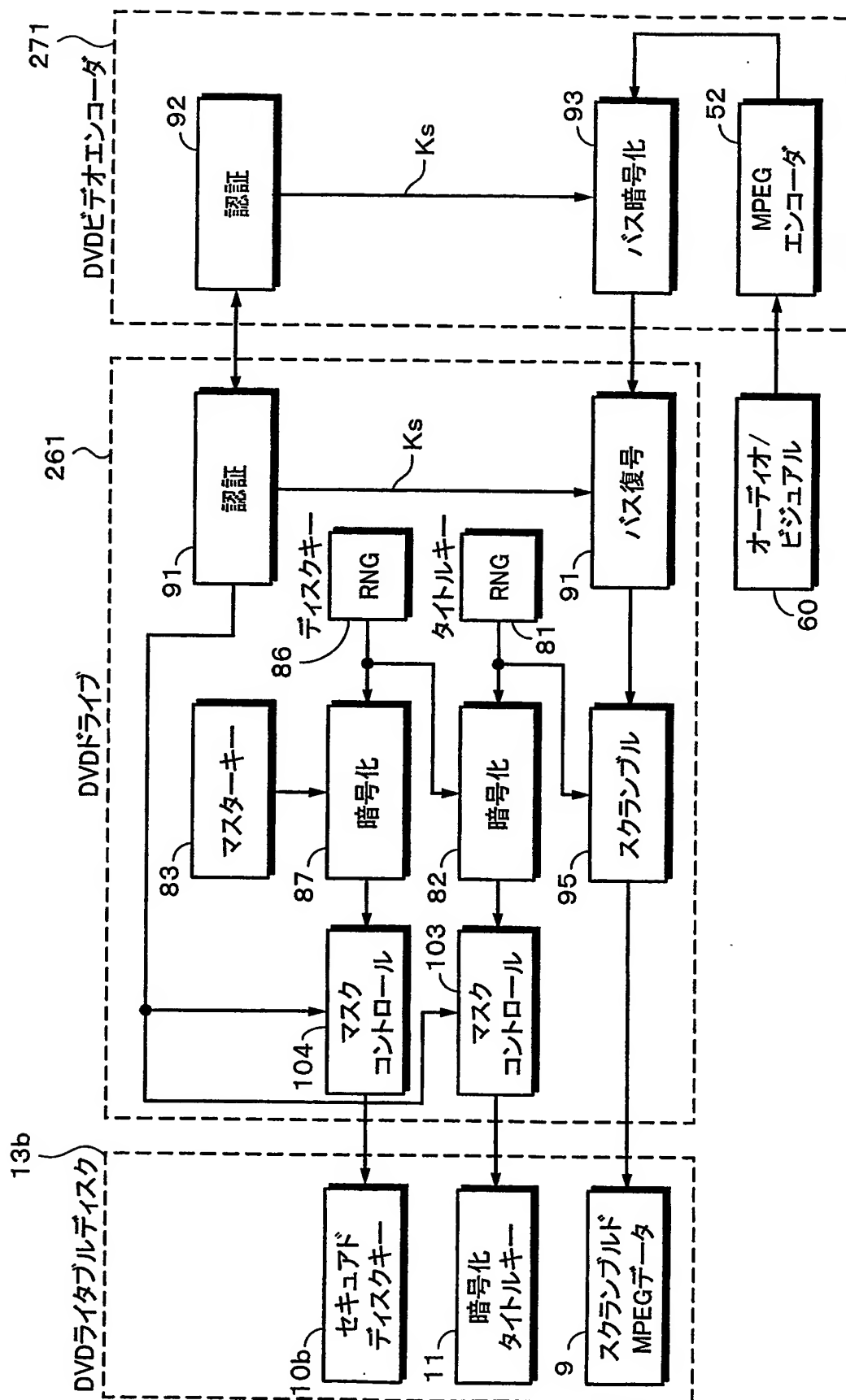


## 第26図

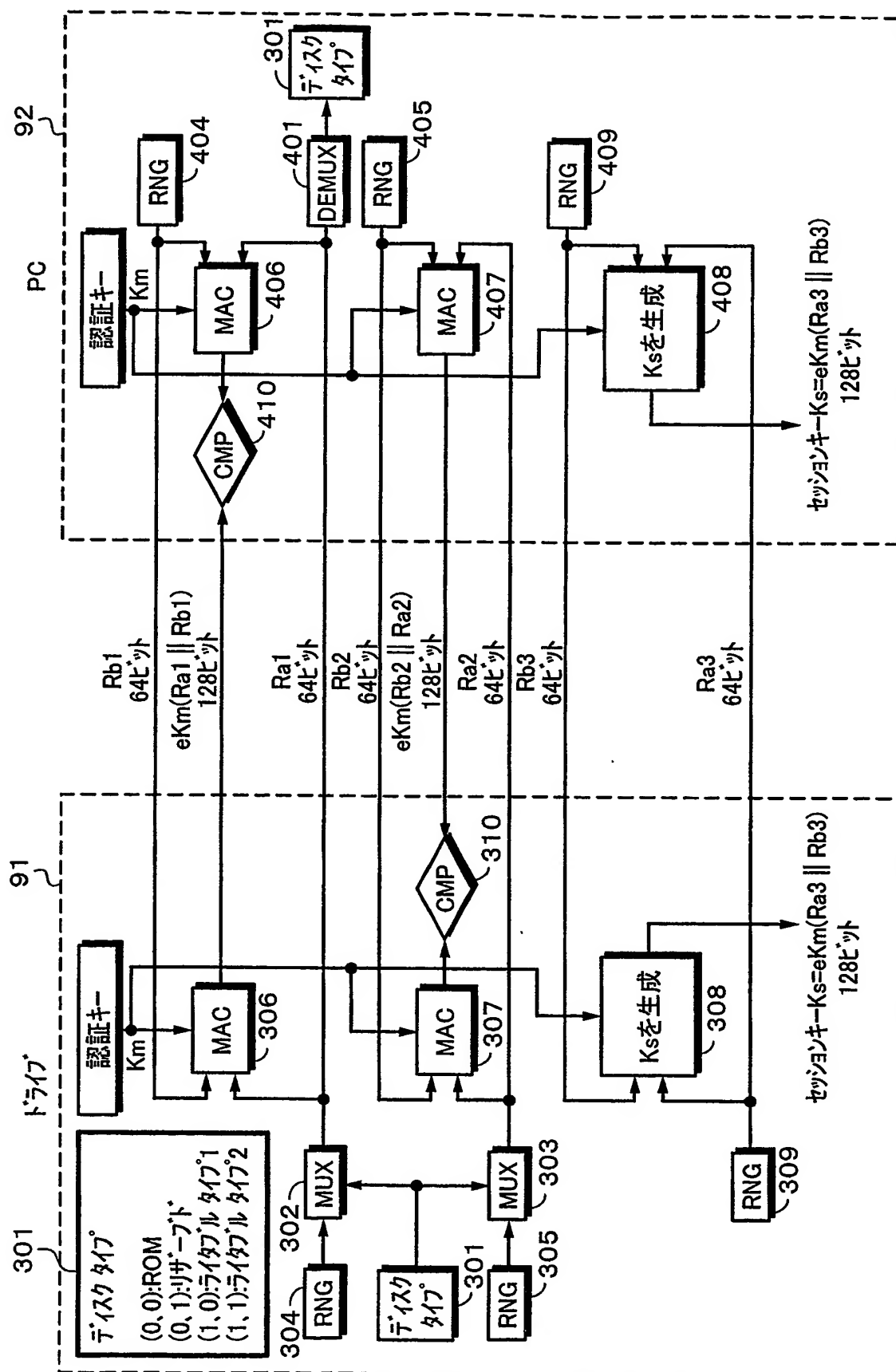




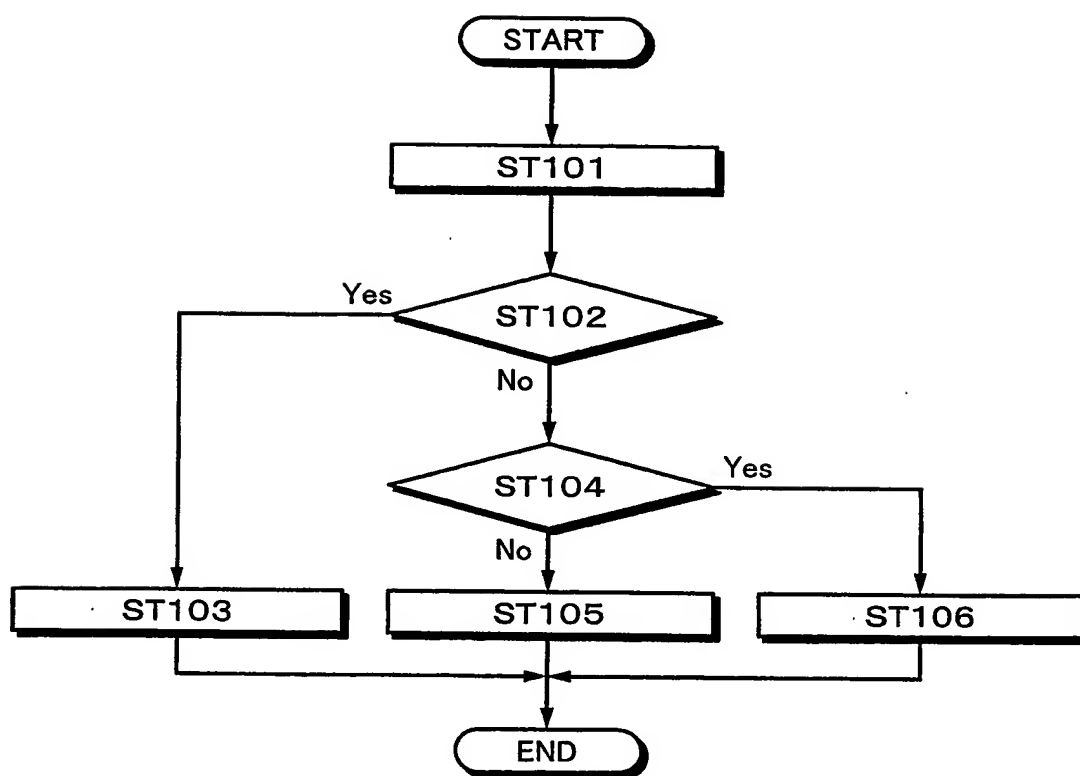
第27図



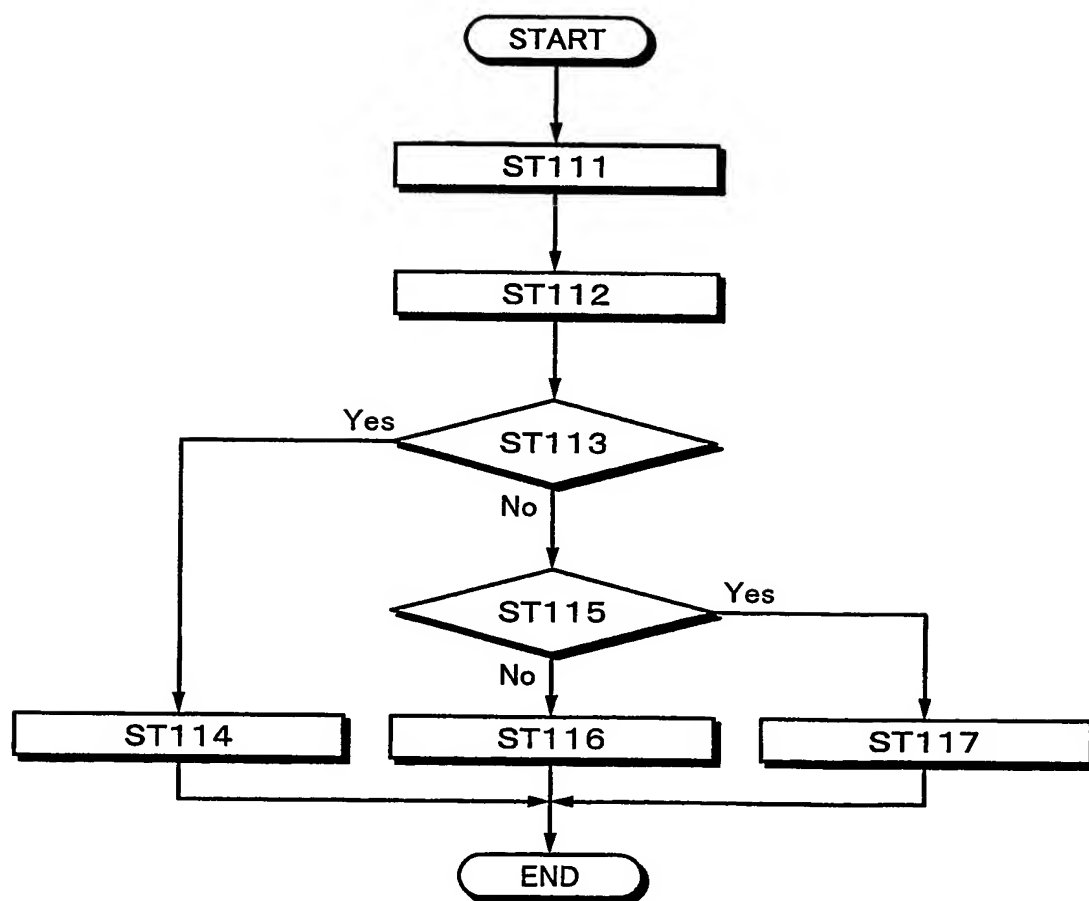
## 第28図



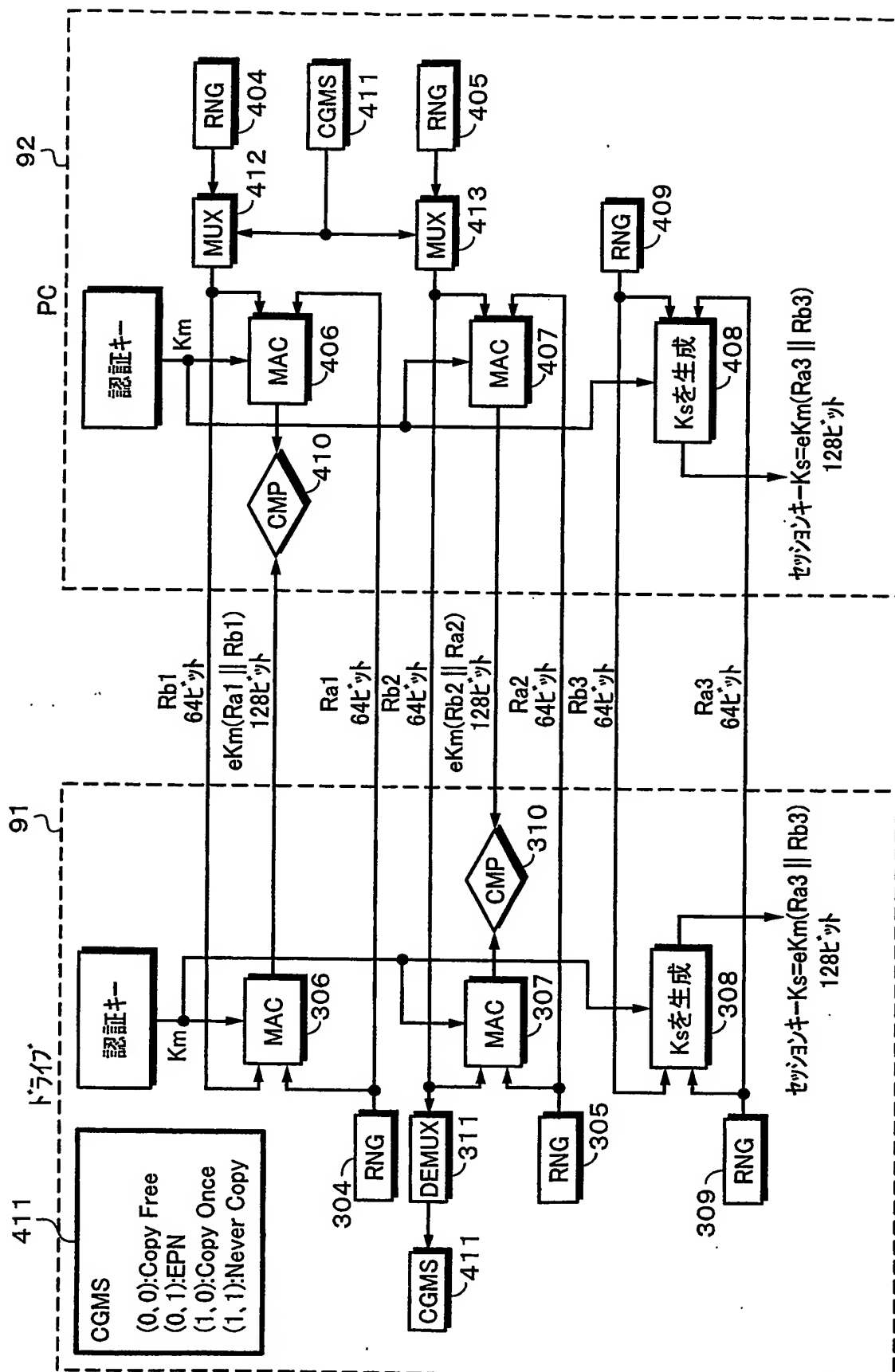
## 第 2 9 図



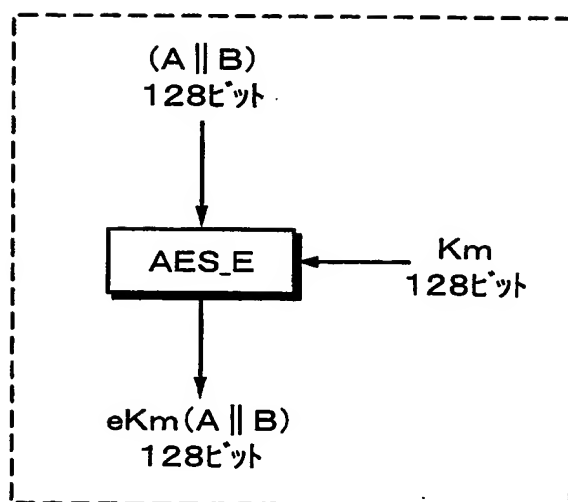
## 第 3 0 図



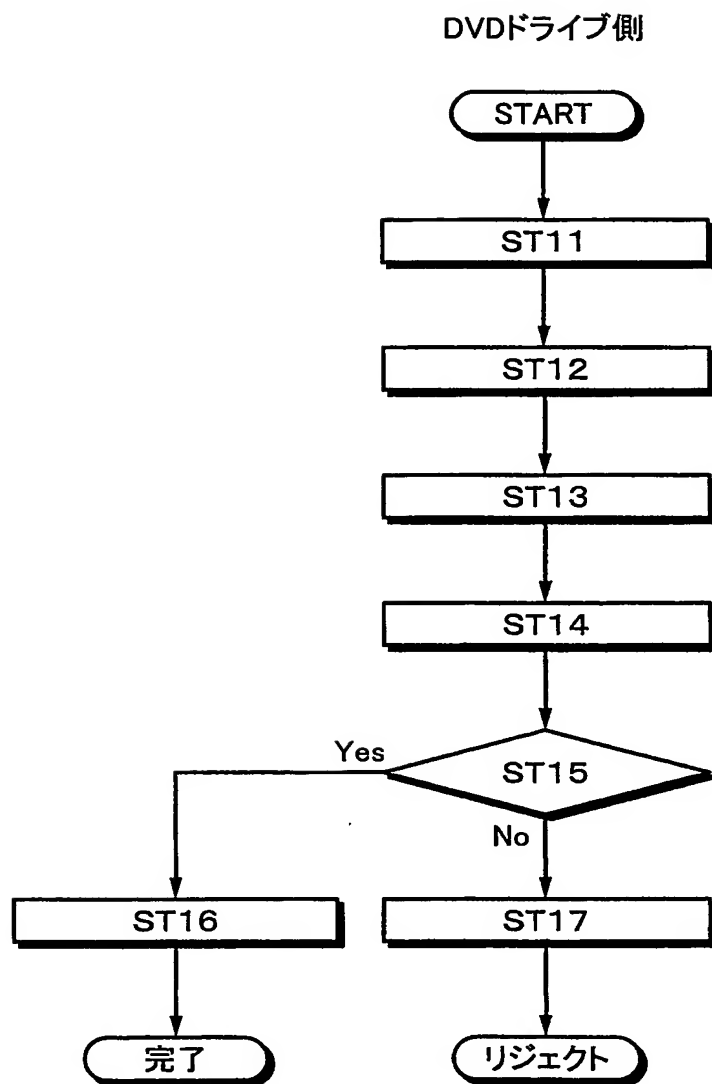
## 第31図



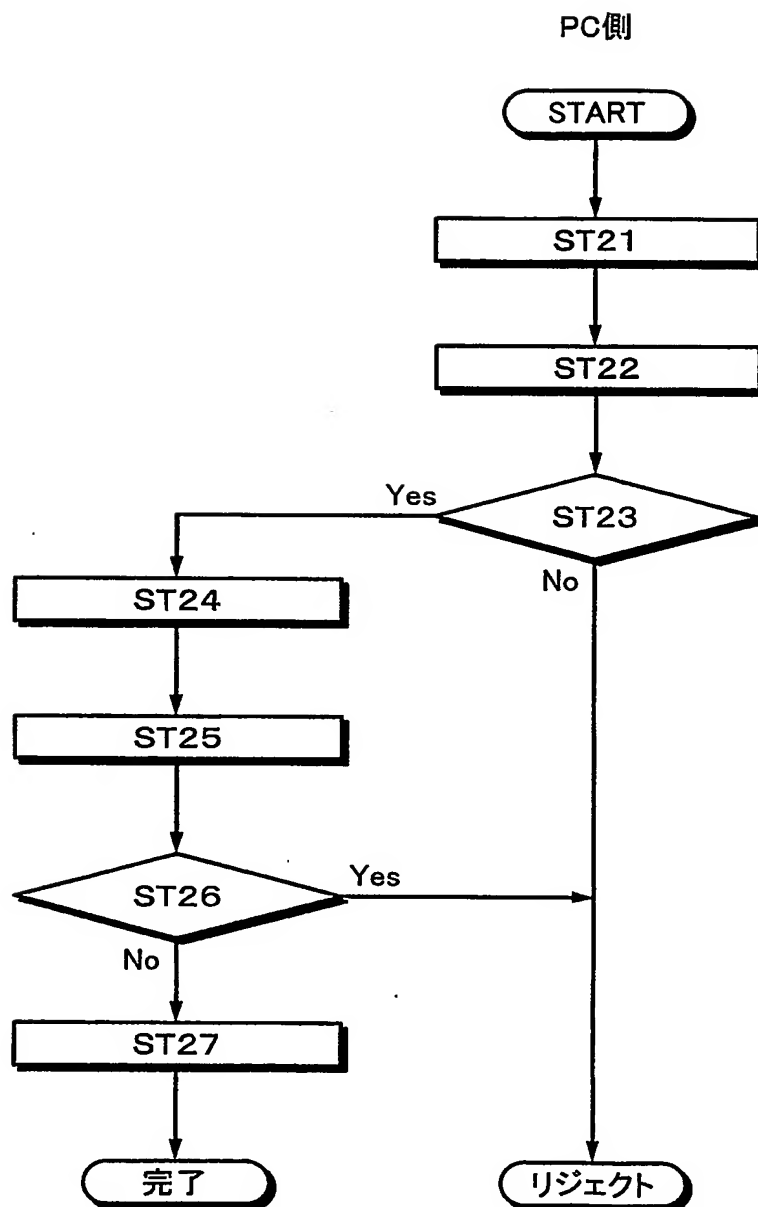
## 第 3 2 図



## 第 3 3 図

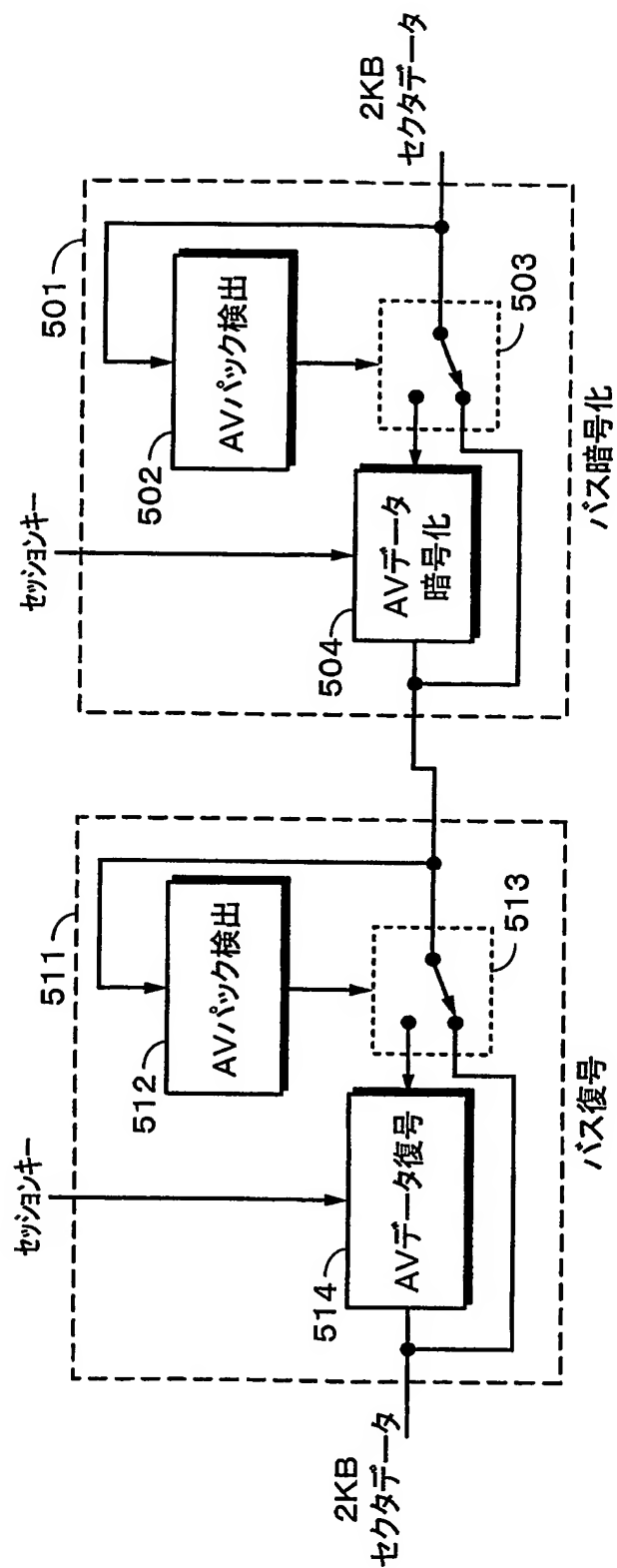


## 第 3 4 図

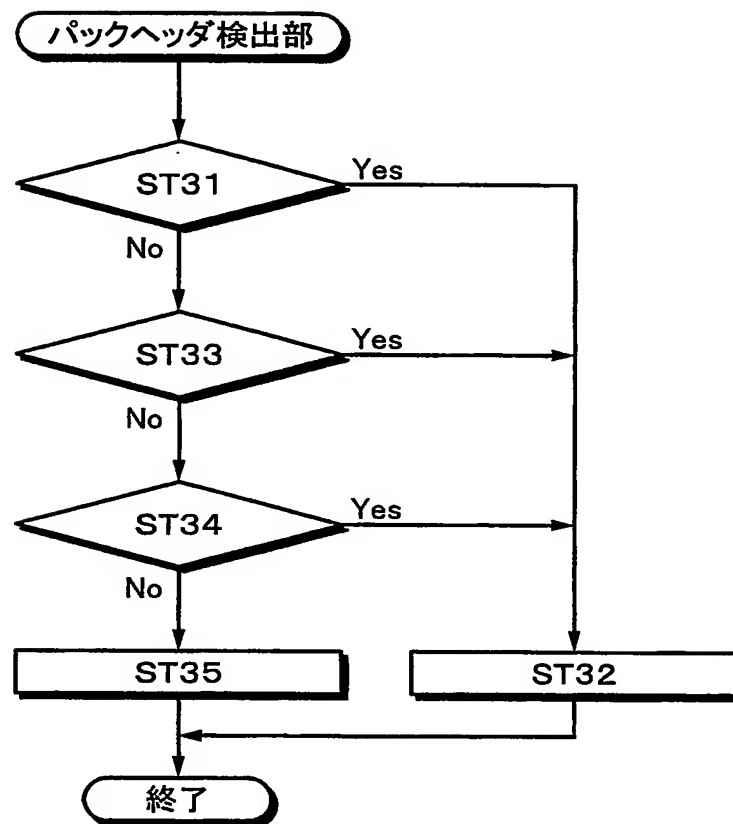




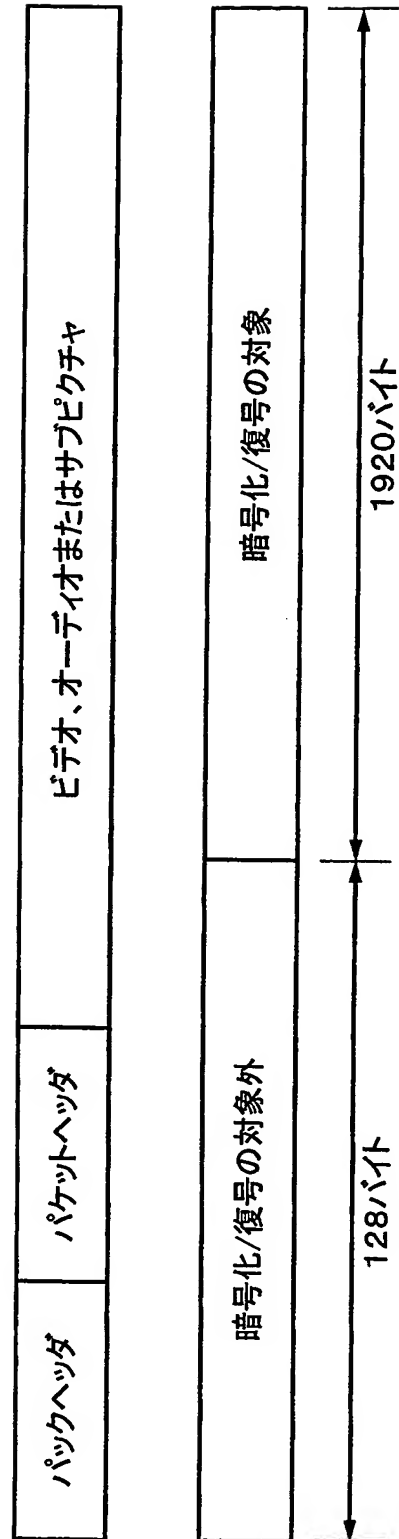
第35図



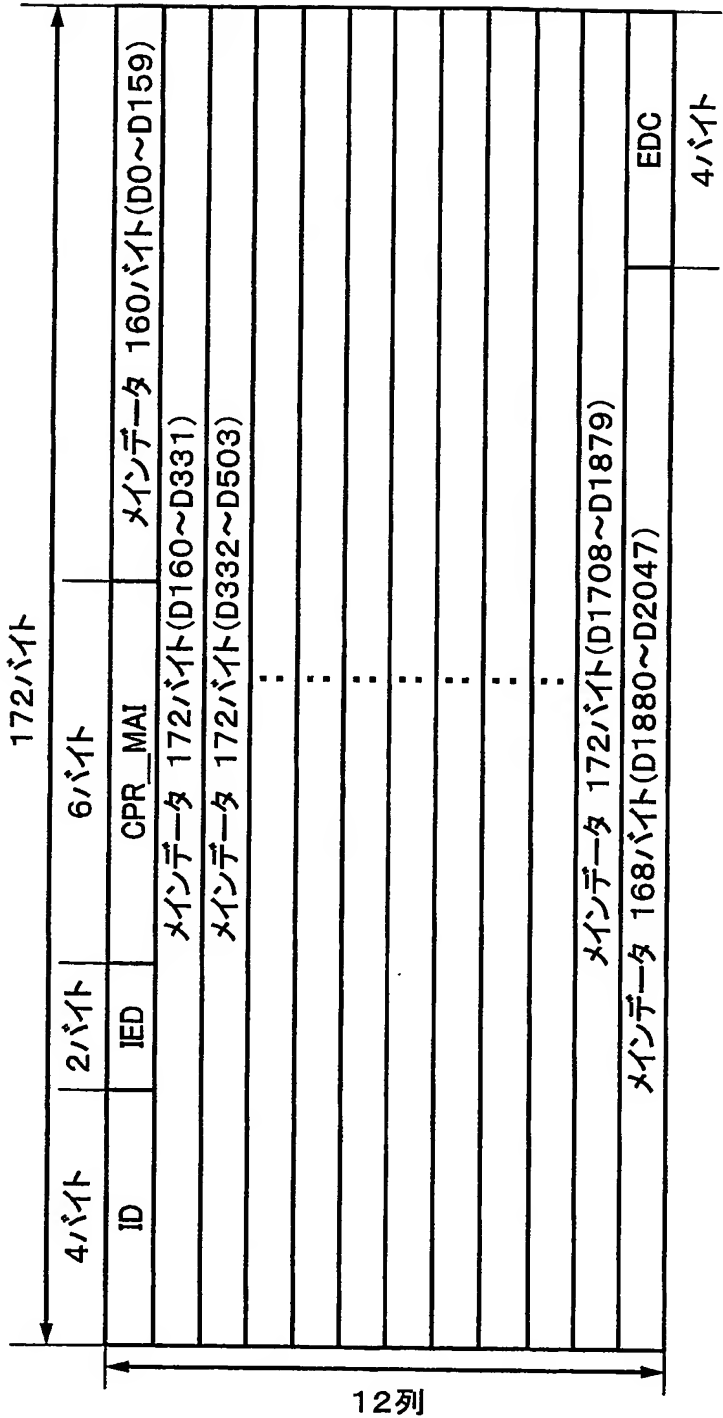
## 第 3 6 図



## 第37図

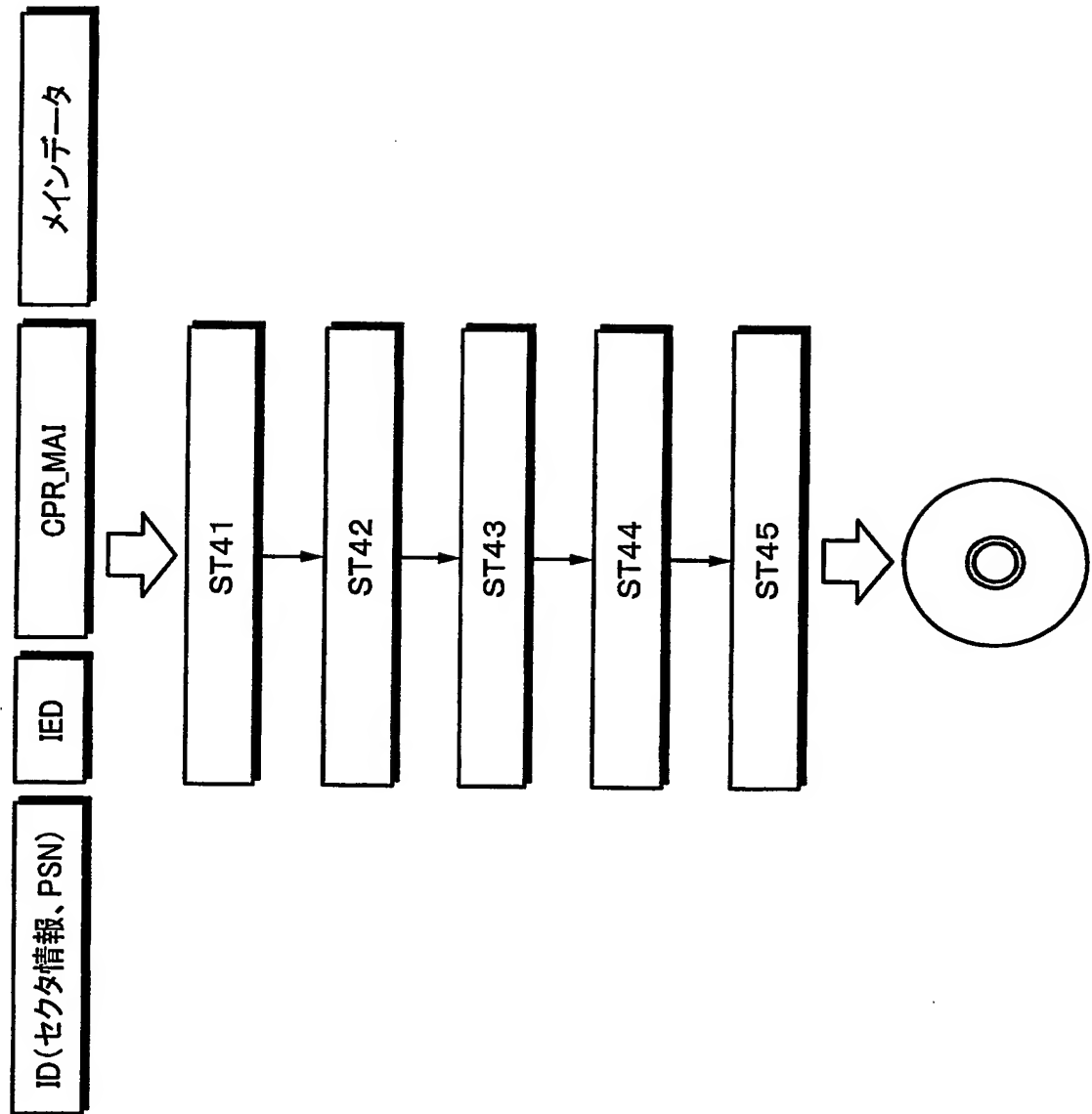


第 38 図

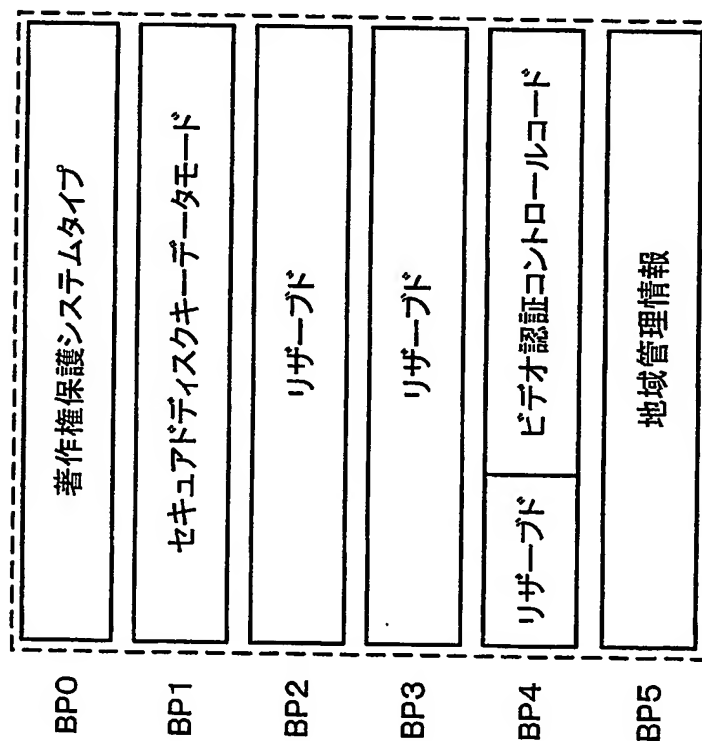


セクタ構成例

第39図



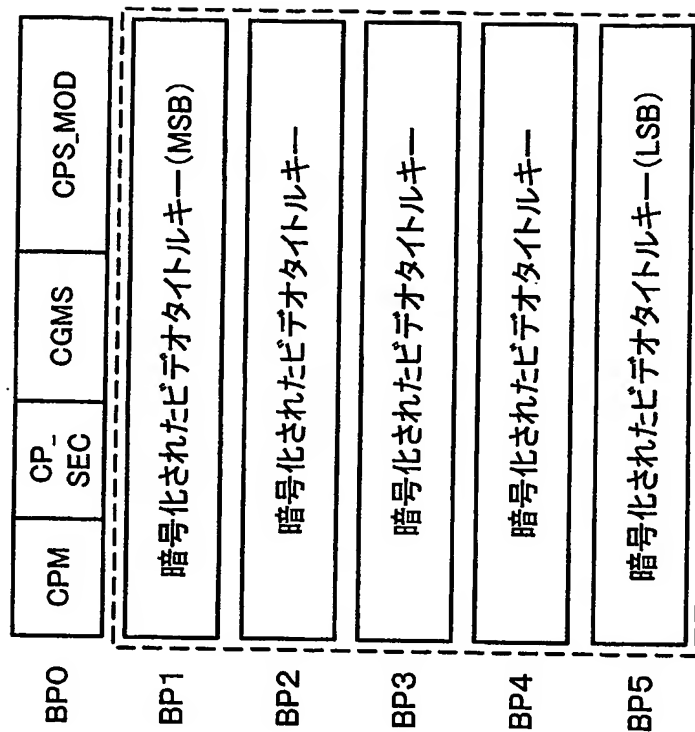
第40図A



リードインエリア内におけるCPR\_MAI

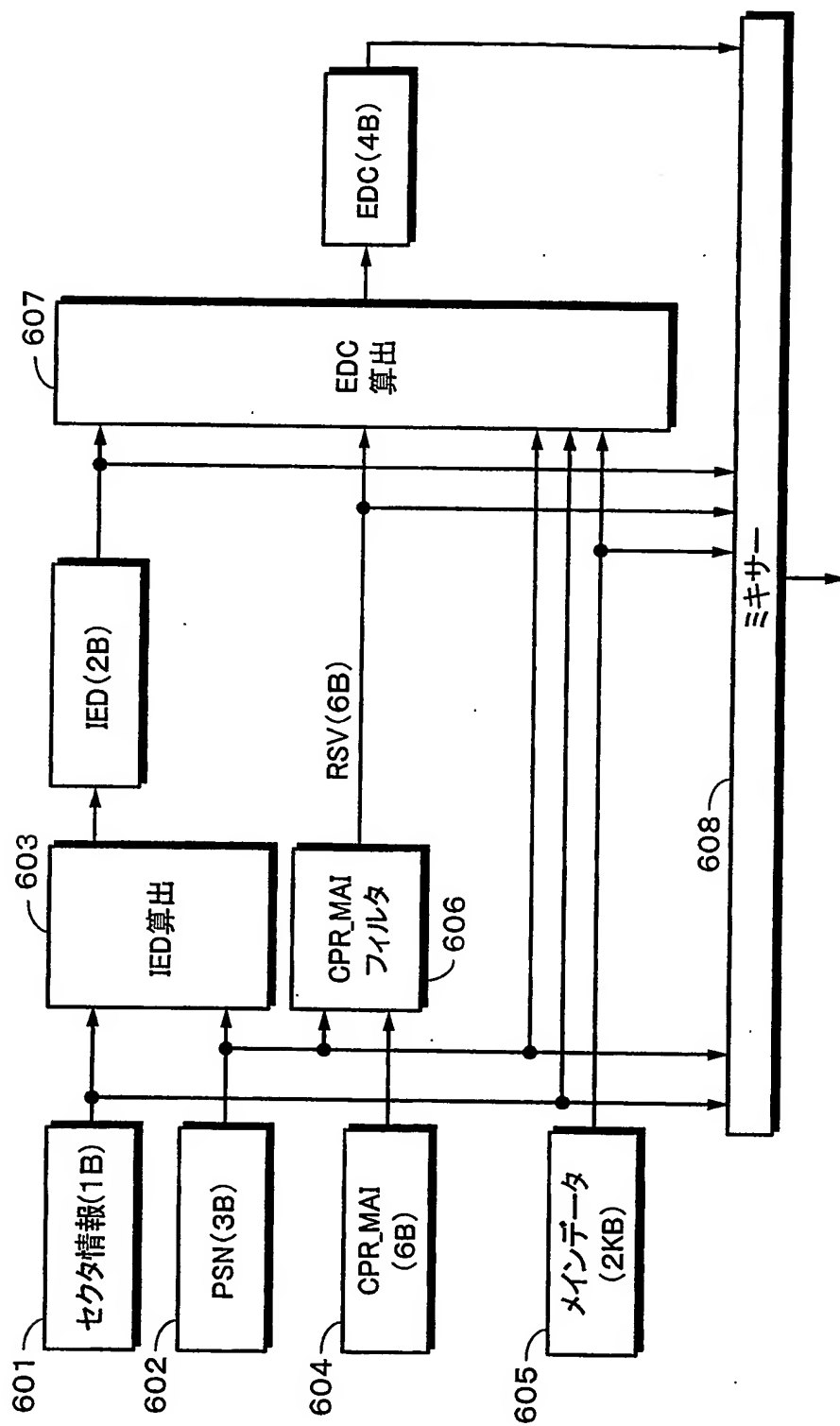
... マスキングエリア

第40図B

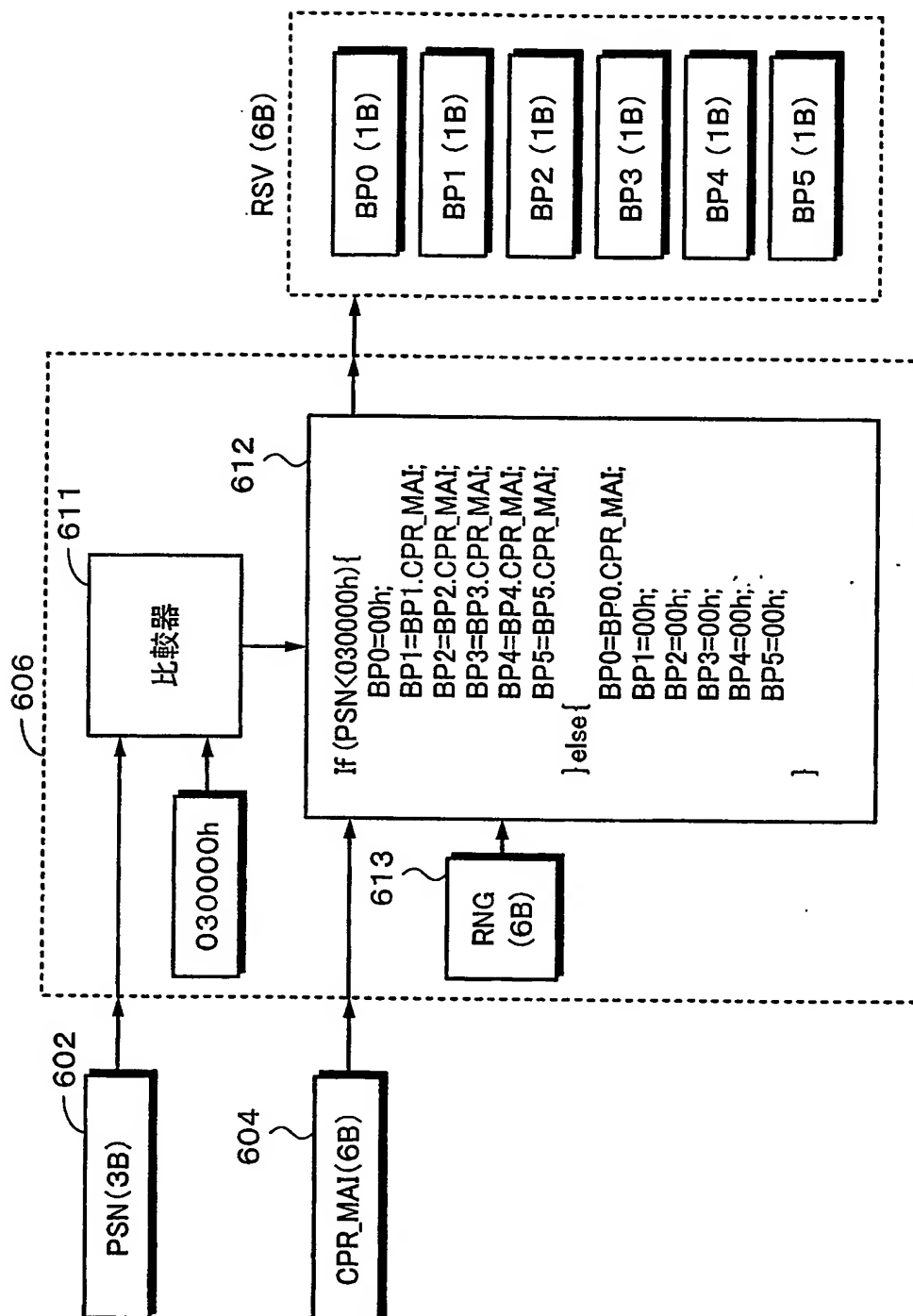


データエリア内におけるCPR\_MAI(CSS)

## 第41図

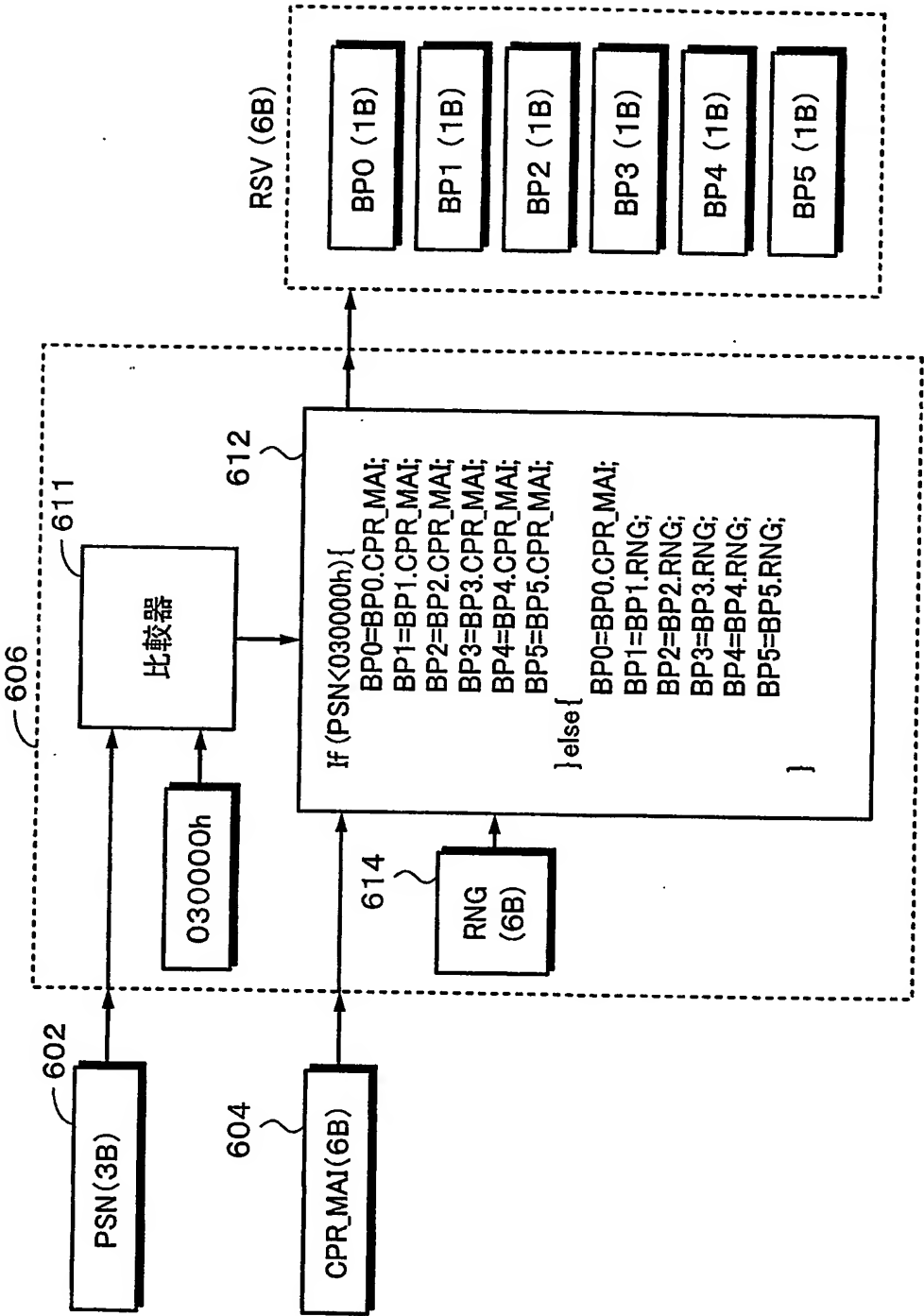


## 第42図

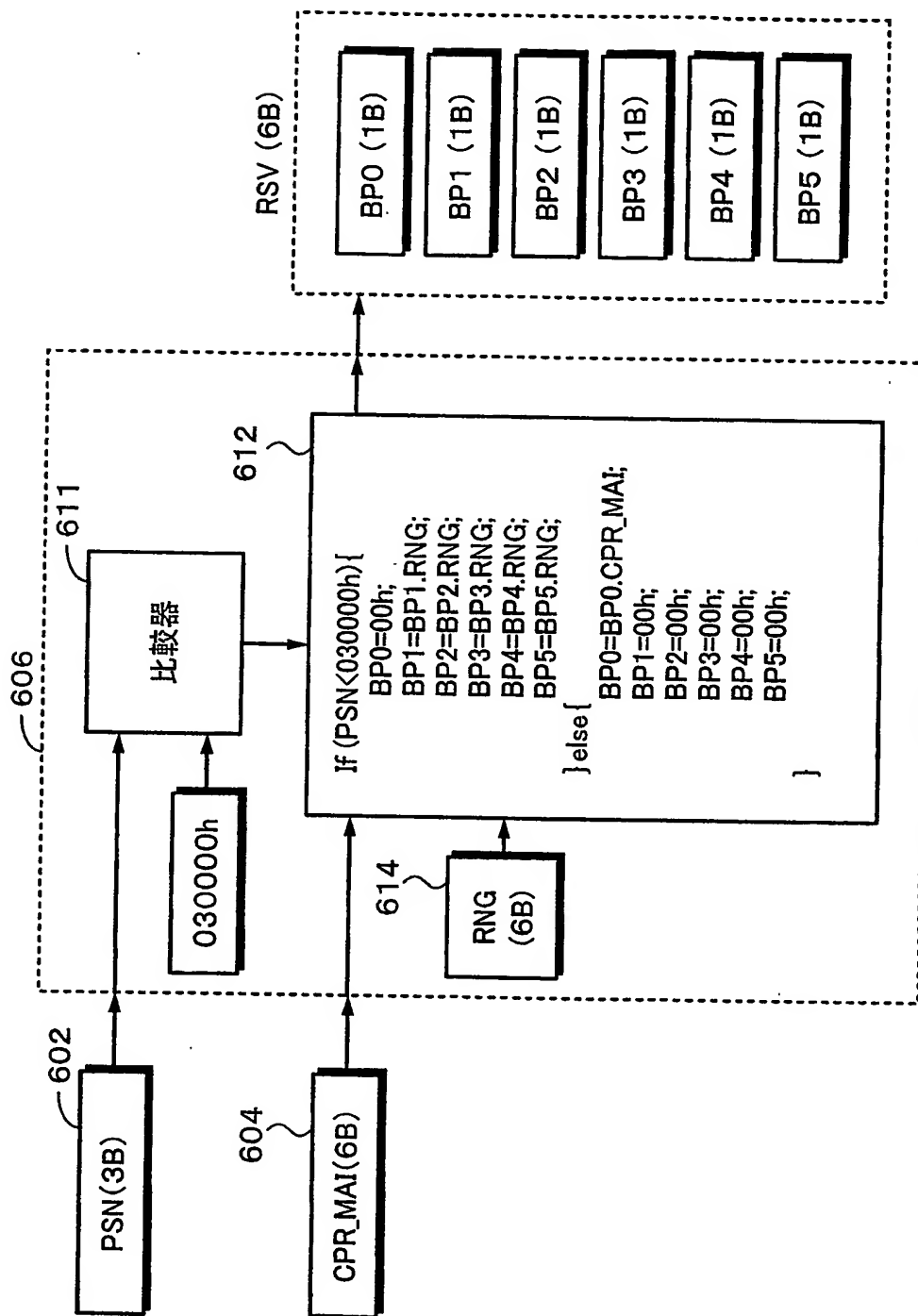




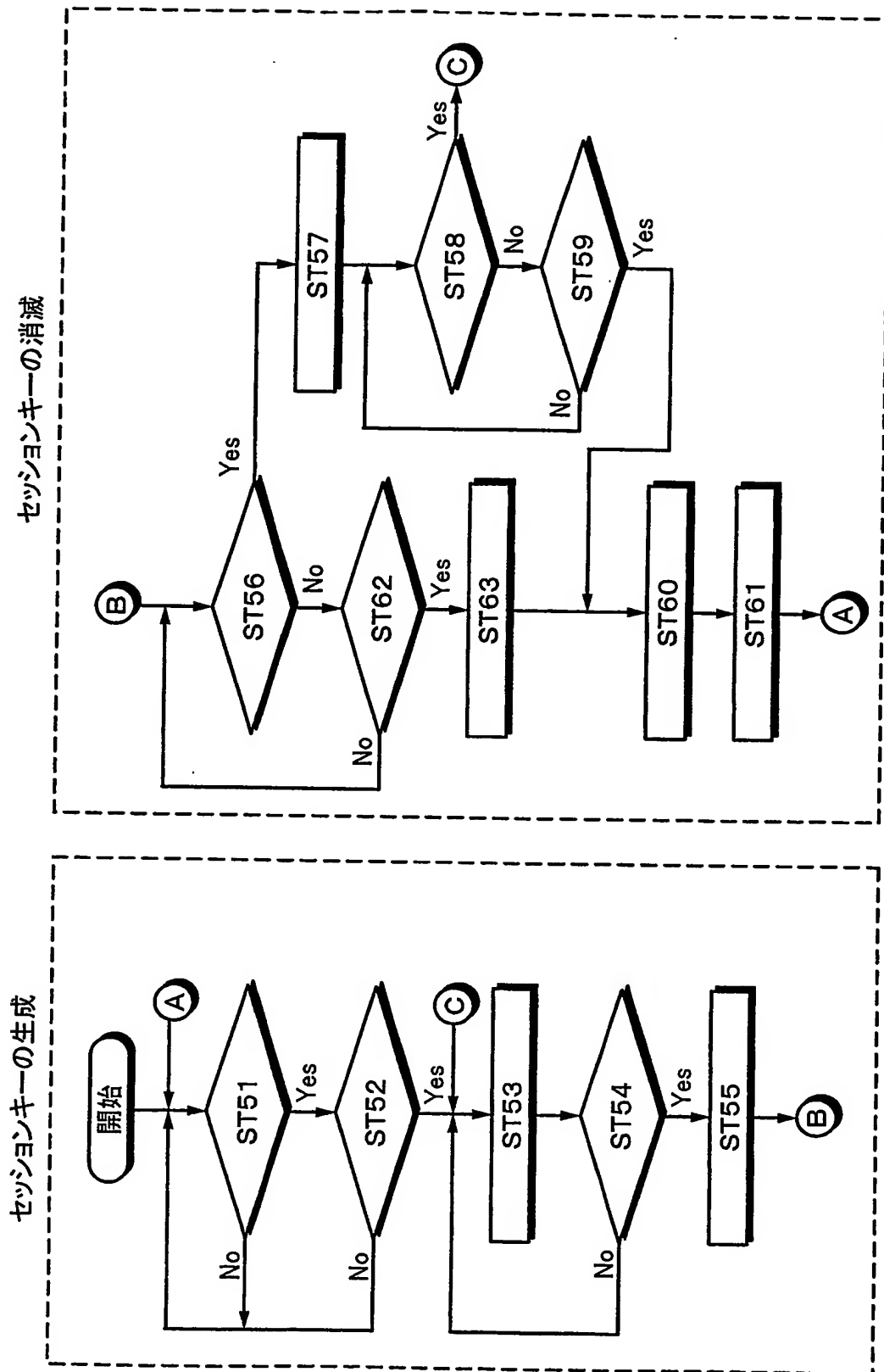
第43図



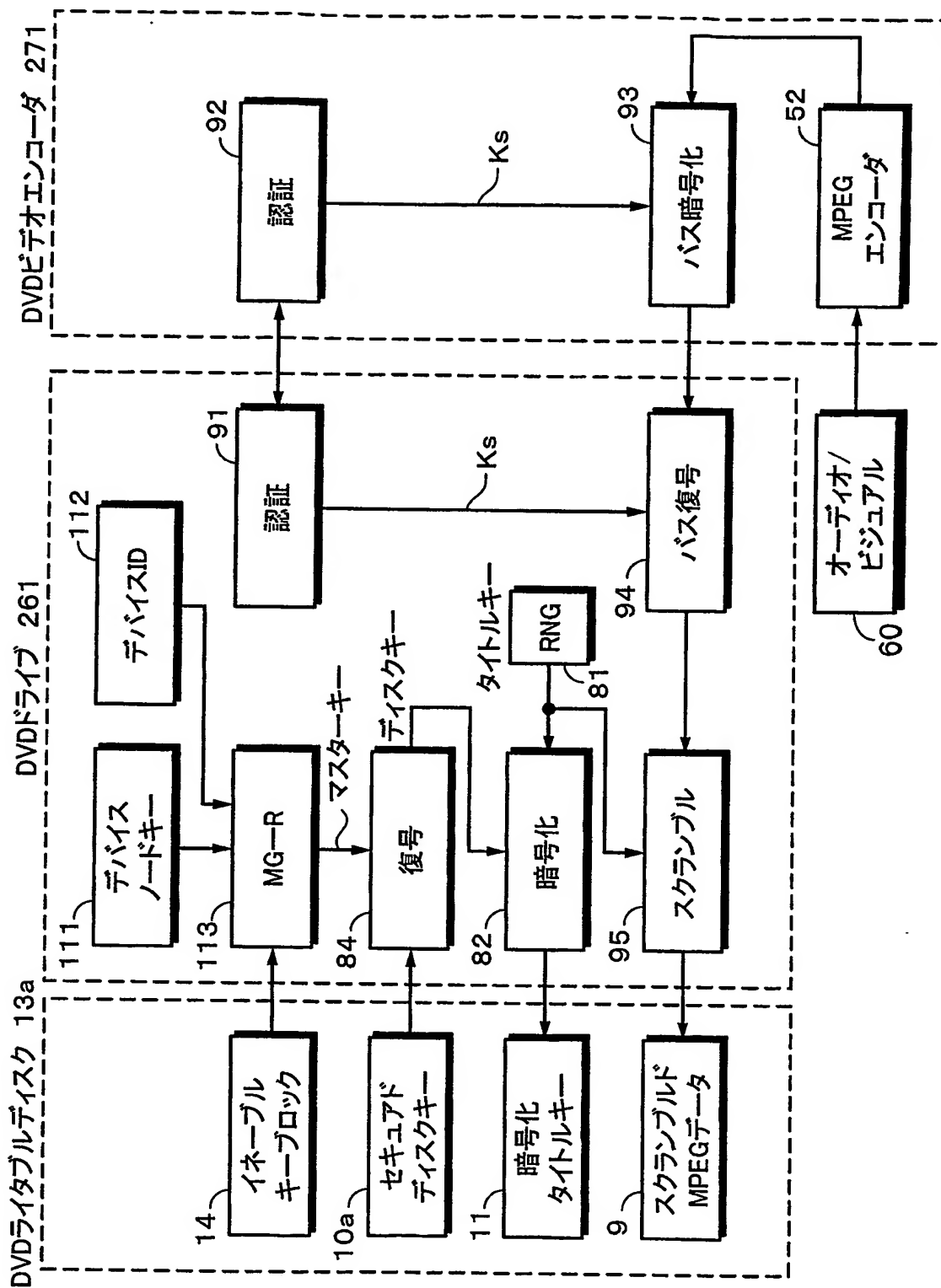
## 第44図



## 第45図



## 第46図



## 符号の説明

- ST101 メディアタイプ判別  
ST102 ROM?  
ST103 ディスクタイプ=ROM  
ST104 ディスクアプリケーションコード=ビデオライタブル?  
ST105 ディスクタイプ=リザーブド  
ST106 ディスクタイプ=ビデオライタブル
- ST111 相互認証  
ST112 ディスクタイプをドライブから取得  
ST113 ディスクタイプ=ROM?  
ST114 データ書き込み禁止  
ST115 ディスクタイプ=ビデオライタブル?  
ST116 データ書き込み可能  
ST117 CSS/CPRMビデオ書き込み可能
- ST11 RECEIVE (Rb1, Rb2)  
ST12 RETURN (eKm (Ra1 || Rb1), Ra1)  
ST13 RETURN (Ra2, Ra3)  
ST14 RECEIVE (eKm (Rb2 || Ra2), Rb3)  
ST15 同一のMAC?  
ST16 セッションキーの確定 (eKm (Ra3 || Rb3))  
ST17 RETURN (エラー)

ST 2 1    S E N D    K E Y ( R b 1 , R b 2 )  
ST 2 2    R E P O R T    K E Y ( e K m ( R a 1 || R b 1 ) , R a 1 )  
ST 2 3    同一のMAC?  
ST 2 4    R E P O R T    K E Y ( R a 2 , R a 3 )  
ST 2 5    S E N D    K E Y ( e K m ( R b 2 || R a 2 ) , R b 3 )  
ST 2 6    エラー?  
ST 2 7    セッションキーの確定 ( e K m ( R a 3 || R b 3 )

ST 3 1    ビデオパック  
ST 3 2    データを暗号化／復号する  
ST 3 3    オーディオパック  
ST 3 4    サブピクチャパック  
ST 3 5    データを暗号化／復号しない

ST 4 1    E D C を加える  
ST 4 2    スクランブルメインデータ  
ST 4 3    E C C の符号化  
ST 4 4    P O を 1 6 列インターリーブ  
ST 4 5    セクタ毎に 2 6 シンクフレーム変調

ST 5 1    D V D + R W / + R ディスク挿入?  
ST 5 2    P C アプリケーション起動?  
ST 5 3    相互認証し、セッションキーを生成  
ST 5 4    完了した?  
ST 5 5    C S S キー書き込み禁止を解除  
ST 5 6    P C アプリケーション終了?

ST 57 PC内で生成したセッションキーを消去  
ST 58 PCアプリケーション起動？  
ST 59 DVD+RW/+Rディスク排出？  
ST 60 ドライブ内で生成したセッションキーを消去  
ST 61 CSSキー書き込み禁止

9	スクランブルドMPEGデータ
10a, 10b	セキュアドディスクキー
11	暗号化タイトルキー
13a, 13b	ライタブルディスク
52	MPEGエンコーダ
53, 95	スクランブラ
56, 78, 84	デクリプタ
57, 83	マスターキー
60	オーディオ／ビジュアルデータ
62, 72	認証部
63, 76, 85	バスエンクリプタ
66, 73, 77	バスデクリプタ
81, 86	乱数発生器
82, 87	エンクリプタ
101, 102	マスクコントロール
161, 261	ドライブ
171, 271	PC

# INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2004/013980

## A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl<sup>7</sup> H04L9/08, H04L12/14, G11B20/10

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl<sup>7</sup> H04L9/08, H04L12/14, G11B20/10

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Toroku Jitsuyo Shinan Koho	1994-2004
Kokai Jitsuyo Shinan Koho	1971-2004	Jitsuyo Shinan Toroku Koho	1996-2004

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	JP 2001-331106 A (Matsushita Electric Industrial Co., Ltd.), 30 November, 2001 (30.11.01), Figs. 2 to 15; Par. Nos. [0076] to [0093] & EP 1134964 A2	1-4, 9-12, 17-19, 23-25, 29-32, 37-40, 45, 47, 49, 51
Y		5-8, 13-16, 20-22, 26-28, 33-36, 41-44, 46, 48, 50, 52

☒ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

\* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search  
08 December, 2004 (08.12.04)

Date of mailing of the international search report  
21 December, 2004 (21.12.04)

Name and mailing address of the ISA/  
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.



## INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2004/013980

## C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 10-210025 A (Matsushita Electric Industrial Co., Ltd.), 07 August, 1998 (07.08.98), Fig. 6; Par. Nos. [0056] to [0065] & EP 840476 A2	5-8, 13-16, 20-22, 26-28, 33-36, 41-44, 46, 48, 50, 52
A	JP 2001-77802 A (Sony Corp.), 23 March, 2001 (23.03.01), Full text (Family: none)	1-52
A	JP 2001-236729 A (Hitachi, Ltd.), 31 August, 2001 (31.08.01), Figs. 5, 7; Par. Nos. [0024] to [0041] & EP 951019 A2	1-52
A	JP 2002-353960 A (Fujitsu Ltd.), 06 December, 2002 (06.12.02), Fig. 10; Par. Nos. [0046] to [0049] & EP 1278114 A2	1-52

## A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl<sup>7</sup> H04L9/08, H04L12/14, G11B20/10

## B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl<sup>7</sup> H04L9/08, H04L12/14, G11B20/10

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1922-1996年

日本国公開実用新案公報 1971-2004年

日本国登録実用新案公報 1994-2004年

日本国実用新案登録公報 1996-2004年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

## C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
X	JP 2001-331106 A (松下電器産業株式会社) 2001. 11. 30, 第2-15図, 【0076】 - 【0093】 段落 & EP 1134964 A2	1-4, 9-12, 17-19, 23-25, 29-32, 37-40, 45, 47, 49, 51 5-8, 13-16, 20-22, 26-28, 33-36, 41-44, 46, 48, 50, 52
Y		

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

## \* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの

「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)

「O」 口頭による開示、使用、展示等に言及する文献

「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&amp;」 同一パテントファミリー文献

国際調査を完了した日

08. 12. 2004

国際調査報告の発送日

21.12.2004

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)

郵便番号100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

石田 信行

5M

9469

電話番号 03-3581-1101 内線 3598

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	JP 10-210025 A (松下電器産業株式会社) 1998. 08. 07, 第6図, 【0056】 - 【0065】 段落 & EP 840476 A2	5-8, 13-16, 20-22, 26-28, 33-36, 41-44, 46, 48, 50, 52
A	JP 2001-77802 A (ソニー株式会社) 2001. 03. 23, 全文 (ファミリーなし)	1 - 52
A	JP 2001-236729 A (株式会社日立製作所) 2001. 08. 31, 第5, 7図, 【0024】 - 【0041】 段落 & EP 951019 A2	1 - 52
A	JP 2002-353960 A (富士通株式会社) 2002. 12. 06, 第10図, 【0046】 - 【0049】 段落 & EP 1278114 A2	1 - 52